PATENT COOPERATION TREATY

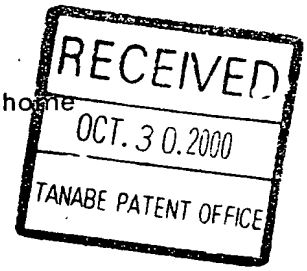
From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:
TANABE, Shigemoto
Green-Fantasia Building
5th floor
11-11-508, Jingumae 1-chome
Shibuya-ku
Tokyo 150-0001
JAPON



Date of mailing (day/month/year) 19 October 2000 (19.10.00)	
Applicant's or agent's file reference S00P0777WO00	**IMPORTANT NOTICE**

International application No.	**International filing date** (day/month/year)	**Priority date** (day/month/year)
PCT/JP00/02290	07 April 2000 (07.04.00)	12 April 1999 (12.04.99)

Applicant
SONY CORPORATION et al

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
   KR,US

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
   CN,EP,SG

   The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
   19 October 2000 (19.10.00) under No. WO 00/62217

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a **demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer
J. Zahra

Telephone No. (41-22) 338.83.38

特　許　協　力　条　約

発信人　日本国特許庁（国際調査機関）

出願人代理人

田辺　恵基　殿

田辺特許 12.6.14 受領

あて名

〒１５０－０００１

東京都渋谷区神宮前１丁目１１番１１－５０８号
グリーンファンタジアビル５階
田辺特許事務所

S745WO

PCT

国際調査報告又は国際調査報告を作成しない旨の決定の送付の通知書

（法施行規則第４１条）
〔ＰＣＴ規則44.1〕

出願人又は代理人の書類記号　S００P０７７７WO０００	発送日（日.月.年）　13.06.00
国際出願番号　ＰＣＴ／ＪＰ００／０２２９０	今後の手続きについては、下記１及び４を参照。
出願人（氏名又は名称）　ソニー株式会社	国際出願日（日.月.年）　０７．０４．００

1．☒ 国際調査報告が作成されたこと、及びこの送付書とともに送付することを、出願人に通知する。
ＰＣＴ１９条の規定に基づく補正書及び説明書の提出
出願人は、国際出願の請求の範囲を補正することができる（ＰＣＴ規則４６参照）。
いつ　補正書の提出期間は、通常国際調査報告の送付の日から２月である。
詳細については添付用紙の備考を参照すること。
どこへ　直接次の場所へ
The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22)740.14.35
詳細な手続については、添付用紙の備考を参照すること。

2．☐ 国際調査報告が作成されないこと、及び法第８条第２項（ＰＣＴ１７条(2)(a)）の規定による国際調査報告を作成しない旨の決定をこの送付書とともに送付することを、出願人に通知する。

3．☐ 法施行規則第４４条（ＰＣＴ規則40.2）に規定する追加手数料の納付に対する異議の申立てに関して、出願人に下記の点を通知する。
☐ 異議の申立てと当該異議についての決定を、その異議の申し立てと当該異議についての決定の両方を指定官庁へ送付することを求める出願人の請求とともに、国際事務局へ送付した。
☐ 当該異議についての決定は、まだ行われていない。決定されしだい出願人に通知する。

4．今後の手続：　出願人は次の点に注意すること。
優先日から１８月経過後、国際出願は国際事務局によりすみやかに国際公開される。出願人が公開の延期を望むときは、国際出願又は優先権の主張の取下げの通知がＰＣＴ規則90の2.1及び90の2.3にそれぞれ規定されているように、国際公開の事務的な準備が完了する前に国際事務局に到達しなければならない。
出願人が優先日から３０月まで（官庁によってはもっと遅く）国内段階の開始を延期することを望むときは、優先日から１９月以内に、国際予備審査の請求書が提出されなければならない。
国際予備審査の請求書若しくは、後にする選択により優先日から１９箇月以内に選択しなかった又は第Ⅱ章に拘束されないため選択できなかったすべての指定官庁に対しては優先日から２０月以内に、国内段階の開始のための所定手続を取らなければならない。

名称及びあて名 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	権限のある職員　５Ｌ　９２８７ 特　許　庁　長　官 電話番号　０３－３５８１－１１０１　内線　３５６２

様式ＰＣＴ／ＩＳＡ／２２０（１９９８年７月）

（添付用紙を参照）

注　　意

1．国際調査報告の発送日から起算する条約第１９条（１）及び規則４６．１に従う国際事務局への補正期間に注意してください。

2．条約２２条（２）に規定する期間に注意してください。

3．文献の写しの請求について

国際調査報告に記載した文献の複写

特許庁にこれらの引用文献の写しを請求することもできますが、日本特許情報機構でもこれらの引用文献の複写物を販売しています。日本特許情報機構に引用文献の複写物を請求する場合は下記の点に注意してください。

〔申込方法〕

（１）特許（実用新案・意匠）公報については、下記の点を明記してください。

○特許・実用新案及び意匠の種類

○出願公告又は出願公開の年次及び番号（又は特許番号、登録番号）

○必要部数

（２）公報以外の文献の場合は、下記の点に注意してください。

○国際調査報告の写しを添付してください（返却します）。

〔申込み及び照会先〕

〒１３５　東京都江東区東陽４－１－７　佐藤ダイヤビル

財団法人　日本特許情報機構　サービス課

ＴＥＬ　０３－５６９０－３９００

注意　特許庁に対して文献の写しの請求をすることができる期間は、国際出願日から７年です。

様式ＰＣＴ／ＩＳＡ／２２０の備考

この備考は、ＰＣＴ１９条の規定に基づく補正書の提出に関する基本的な指示を与えるためのものである。この備考は特許協力条約並びにこの条約に基づく規則及び実施細則の規定に基づいている。この備考とそれらの規定とが相違する場合には、後者が適用される。詳細な情報については、ＷＩＰＯの出版物であるＰＣＴ出願人の手引も参照すること。

ＰＣＴ１９条の規定に基づく補正書の提出に関する指示

出願人は、国際調査報告を受領した後、国際出願の請求の範囲を補正する機会が一回ある。しかし、国際出願のすべての部分（請求の範囲、明細書及び図面）が、国際予備審査の手続においても補正できるもので、例えば出願人が仮保護のために補正書を公開することを希望する場合又は国際公開前に請求の範囲を補正する別の理由がある場合を除き、通常ＰＣＴ１９条の規定に基づく補正書を提出する必要はないことを強調しておく。さらに、仮保護は一部の国のみで与えられるだけであることも強調しておく。

補正の対象となるもの

ＰＣＴ１９条の規定により請求の範囲のみ補正することができる。
国際段階においてＰＣＴ３４条の規定に基づく国際予備審査の手続きにおいて請求の範囲を（更に）補正することができる。
明細書及び図面は、ＰＣＴ３４条の規定に基づく国際予備審査の手続においてのみ補正することができる。
国内段階に移行する際、ＰＣＴ２８条（又はＰＣＴ４１条）の規定により、国際出願のすべての部分を補正することができる。

いつ

国際調査報告の送付の日から２月又は優先日から１６月の内どちらか遅く満了するほうの期間内。しかし、その期間の満了後であっても国際公開の技術的な準備の完了前に国際事務局が補正を受領した場合には、その補正書は、期間内に受理されたものとみなすことを強調しておく（ＰＣＴ規則46.1）。

補正書を提出すべきところ

補正書は、国際事務局のみに提出でき、受理官庁又は国際調査機関には提出してはいけない（ＰＣＴ規則46.2）。
国際予備審査の請求書を提出した／する場合については、以下を参照すること。

どのように

１以上の請求の範囲の削除、１以上の新たな請求の範囲の追加、又は１以上の請求の範囲の記載の補正による。
差替え用紙は、補正の結果、出願当初の用紙と相違する請求の範囲の各用紙毎に提出する。
差替え用紙に記載されているすべての請求の範囲には、アラビア数字を付さなければならない。請求の範囲を削除する場合、その他の請求の範囲の番号を付け直す必要はない。請求の範囲の番号を付け直す場合には、連続番号で付け直さなければならない（ＰＣＴ実施細則第205号(b)）。
補正は国際公開の言語で行う。

補正書にどのような書類を添付しなければならないか

書簡（ＰＣＴ実施細則第205号(b)）

補正書には書簡を添付しなければならない。
書簡は国際出願及び補正された請求の範囲とともに公開されることはない。これを「ＰＣＴ１９条(1)に規定する説明書」と混同してはならない（「ＰＣＴ１９条(1)に規定する説明書」については、以下を参照）。
書簡は、英語又は仏語を選択しなければならない。ただし、国際出願の言語が英語の場合、書簡は英語で、仏語の場合、書簡は仏語で記載しなければならない。
書簡には、出願時の請求の範囲と補正された請求の範囲との相違について表示しなければならない。特に、国際出願に記載した各請求の範囲との関連で次の表示（２以上の請求の範囲についての同一の表示する場合は、まとめることができる。）をしなければならない。
(i) この請求の範囲は変更しない。
(ii) この請求の範囲は削除する。
(iii) この請求の範囲は追加である。
(iv) この請求の範囲は出願時の１以上の請求の範囲と差し替える。
(v) この請求の範囲は出願時の請求の範囲の分割の結果である。

次に、添付する書簡中での、補正についての説明の例を示す。

１．［請求の範囲の一部の補正によって請求の範囲の項数が４８から５１になった場合］：
“請求の範囲１－２９、３１、３２、３４、３５、３７－４８項は、同じ番号のもとに補正された請求の範囲と置き換えられた。請求の範囲３０、３３及び３６項は変更なし。新たに請求の範囲４９－５１項が追加された。”
２．［請求の範囲の全部の補正によって請求の範囲の項数が１５から１１になった場合］：
“請求の範囲１－１５項は、補正された請求の範囲１－１１項に置き換えられた。”
３．［原請求の範囲の項数が１４で、補正が一部の請求の範囲の削除と新たな請求の範囲の追加を含む場合］：
“請求の範囲１－６及び１４項は変更なし。請求の範囲７－１３は削除。新たに請求の範囲１５、１６及び１７項を追加。”又は
“請求の範囲７－１３は削除。新たに請求の範囲１５、１６及び１７項を追加。その他の全ての請求の範囲は変更なし。”
４．［各種の補正がある場合］：
“請求の範囲１－１０項は変更なし。請求の範囲１１－１３、１８及び１９項は削除。請求の範囲１４、１５及び１６項は補正された請求の範囲１４項に置き換えられた。請求の範囲１７項は補正された請求の範囲１５、１６及び１７項に分割された。新たに請求の範囲２０及び２１項が追加された。”

“ＰＣＴ１９条(1)の規定に基づく説明書”（ＰＣＴ規則46.4）

補正書には、補正並びにその補正が明細書及び図面に与える影響についての説明書を提出することができる（明細書及び図面はＰＣＴ１９条(1)の規定に基づいては補正できない）。

説明書は、国際出願及び補正された請求の範囲とともに公開される。

説明書は、国際公開の言語で作成しなければならない。

説明書は、簡潔でなければならず、英語の場合又は英語に翻訳した場合に５００語を越えてはならない。

説明書は、出願時の請求の範囲と補正された請求の範囲との相違を示す書簡と混同してはならない。説明書を、その書簡に代えることはできない。説明書は別紙で提出しなければならず、見出しを付すものとし、その見出しは“ＰＣＴ１９条(1)の規定に基づく説明書”の語句を用いることが望ましい。

説明書には、国際調査報告又は国際調査報告に列記された文献との関連性に関して、これらを誹謗する意見を記載してはならない。国際調査報告に列記された特定の請求の範囲に関連する文献についての言及は、当該請求の範囲の補正に関してのみ行うことができる。

国際予備審査の請求書が提出されている場合

ＰＣＴ１９条の規定に基づく補正書及び添付する説明書の提出の時に国際予備審査の請求書が既に提出されている場合には、出願人は、補正書（及び説明書）を国際事務局に提出すると同時にその写し及び必要な場合、その翻訳文を国際予備審査機関にも提出することが望ましい（ＰＣＴ規則55.3(a)、62.2の第１文を参照）。詳細は国際予備審査請求書（ＰＣＴ／ＩＰＥＡ／４０１）の注意書参照。

国内段階に移行するための国際出願の翻訳に関して

国内段階に移行する際、ＰＣＴ１９条の規定に基づいて補正された請求の範囲の翻訳を出願時の請求の範囲の翻訳の代わりに又は追加して、指定官庁／選択官庁に提出しなければならないこともあるので、出願人は注意されたい。

指定官庁／選択官庁の詳細な要求については、ＰＣＴ出願人の手引きの第Ⅱ巻を参照。

特　許　協　力　条　約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　S00P0777WO00	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０２２９０	国際出願日（日.月.年）　０７．０４．００	優先日（日.月.年）　１２．０４．９９
出願人（氏名又は名称）　ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　2　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ｉ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　１３　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０２２９０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int. Cl⁷ G06F17/60

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int. Cl⁷ G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1926-1996年
日本国公開実用新案公報　1971-2000年
日本国実用新案登録公報　1996-2000年
日本国登録実用新案公報　1994-2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTファイル(JOIS)

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO, 96/27155, A2(InerTrust Technologies Corp.)6.9月.1996(06.09.96)&JP, 10-512074, A	1-8
Y	人文科学とコンピュータ，第36-8巻，11月.1997 河原正治「著作権処理技術の最近の動向」p.43-48	1-8

☐ Ｃ欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
24.05.00	13.06.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	岩間　直純	5L	9287
	電話番号　０３－３５８１－１１０１　内線　3562		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF RECEIPT OF RECORD COPY

(PCT Rule 24.2(a))

To:

TANABE, Shigemoto
Green-Fantasia Building
5th floor
11-11-508, Jingumae 1-chome
Shibuya-ku
Tokyo 150-0001
JAPON

RECEIVED
JUN. 13. 2000
TANABE PATENT OFFICE

Date of mailing (day/month/year)	IMPORTANT NOTIFICATION
01 May 2000 (01.05.00)	
Applicant's or agent's file reference	**International application No.**
S00P0777WO00	PCT/JP00/02290

The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

SONY CORPORATION (for all designated States except US)
ISHIBASHI, Yoshihito (for US)

International filing date	:	07 April 2000 (07.04.00)
Priority date(s) claimed	:	12 April 1999 (12.04.99)
Date of receipt of the record copy by the International Bureau	:	26 April 2000 (26.04.00)
List of designated Offices	:	

EP :DE,FR,GB
National :CN,KR,SG,US

ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- [X] time limits for entry into the national phase
- [X] confirmation of precautionary designations
- [X] requirements regarding priority documents

A copy of this Notification is being sent to the receiving Office and to the International Searching Authority.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer:

Y. KUWAHARA

Telephone No. (41-22) 338.83.38

003253937

INFORMATION ON TIME LIMITS FOR ENTERING THE NATIONAL PHASE

The applicant is reminded that the "national phase" must be entered before each of the designated Offices indicated in the Notification of Receipt of Record Copy (Form PCT/IB/301) by paying national fees and furnishing translations, as prescribed by the applicable national laws.

The time limit for performing these procedural acts is **20 MONTHS** from the priority date or, for those designated States which the applicant elects in a demand for international preliminary examination or in a later election, **30 MONTHS** from the priority date, provided that the election is made before the expiration of 19 months from the priority date. Some designated (or elected) Offices have fixed time limits which expire even later than 20 or 30 months from the priority date. In other Offices an extension of time or grace period, in some cases upon payment of an additional fee, is available.

In addition to these procedural acts, the applicant may also have to comply with other special requirements applicable in certain Offices. **It is the applicant's responsibility** to ensure that the necessary steps to enter the national phase are taken in a timely fashion. Most designated Offices do not issue reminders to applicants in connection with the entry into the national phase.

For detailed information about the procedural acts to be performed to enter the national phase before each designated Office, the applicable time limits and possible extensions of time or grace periods, and any other requirements, see the relevant Chapters of Volume II of the PCT Applicant's Guide. Information about the requirements for filing a demand for international preliminary examination is set out in Chapter IX of Volume I of the PCT Applicant's Guide.

GR and ES became bound by PCT Chapter II on 7 September 1996 and 6 September 1997, respectively, and may, therefore, be elected in a demand or a later election filed on or after 7 September 1996 and 6 September 1997, respectively, regardless of the filing date of the international application. (See second paragraph above.)

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

CONFIRMATION OF PRECAUTIONARY DESIGNATIONS

This notification lists only specific designations made under Rule 4.9(a) in the request. It is important to check that these designations are correct. Errors in designations can be corrected where precautionary designations have been made under Rule 4.9(b). The applicant is hereby reminded that any precautionary designations may be confirmed according to Rule 4.9(c) before the expiration of 15 months from the priority date. If it is not confirmed, it will automatically be regarded as withdrawn by the applicant. There will be no reminder and no invitation. Confirmation of a designation consists of the filing of a notice specifying the designated State concerned (with an indication of the kind of protection or treatment desired) and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.

REQUIREMENTS REGARDING PRIORITY DOCUMENTS

For applicants who have not yet complied with the requirements regarding priority documents, the following is recalled.

Where the priority of an earlier national, regional or international application is claimed, the applicant must submit a copy of the said earlier application, certified by the authority with which it was filed ("the priority document") to the receiving Office (which will transmit it to the International Bureau) or directly to the International Bureau, before the expiration of 16 months from the priority date, provided that any such priority document may still be submitted to the International Bureau before that date of international publication of the international application, in which case that document will be considered to have been received by the International Bureau on the last day of the 16-month time limit (Rule 17.1(a)).

Where the priority document is issued by the receiving Office, the applicant may, instead of submitting the priority document, request the receiving Office to prepare and transmit the priority document to the International Bureau. Such request must be made before the expiration of the 16-month time limit and may be subjected by the receiving Office to the payment of a fee (Rule 17.1(b)).

If the priority document concerned is not submitted to the International Bureau or if the request to the receiving Office to prepare and transmit the priority document has not been made (and the corresponding fee, if any, paid) within the applicable time limit indicated under the preceding paragraphs, any designated State may disregard the priority claim, provided that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity to furnish the priority document within a time limit which is reasonable under the circumstances.

Where several priorities are claimed, the priority date to be considered for the purposes of computing the 16-month time limit is the filing date of the earliest application whose priority is claimed.

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING SUBMISSION OR TRANSMITTAL OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

TANABE, Shigemoto
Green-Fantasia Building
5th floor
11-11-508, Jingumae 1-chome
Shibuya-ku
Tokyo 150-0001
JAPON

S745WO

RECEIVED
JUN. 27. 2000
TANABE PATENT OFFICE

Date of mailing (day/month/year) 08 June 2000 (08.06.00)	
Applicant's or agent's file reference S00P0777WO00	**IMPORTANT NOTIFICATION**
International application No. PCT/JP00/02290	International filing date (day/month/year) 07 April 2000 (07.04.00)
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 12 April 1999 (12.04.99)
Applicant SONY CORPORATION et al	

1. The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).

2. This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.

3. An **asterisk(*)** appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

4. The **letters "NR"** appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
12 Apri 1999 (12.04.99)	11/103992	JP	26 May 2000 (26.05.00)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer

Somsak Thiphrakesone

Telephone No. (41-22) 338.83.38

特許協力条約に基づく国際出願

願　　書

出願人は、この国際出願が特許協力条約に従って処理されることを請求する。

受理官庁記入欄

国際出願番号

国際出願日　07.4.'00 PCT 受領印

（受付印）

控

出願人又は代理人の書類記号（希望する場合、最大12字）　S00P0777WO00

第I欄　発明の名称

情報処理装置および方法、並びに提供媒体

第II欄　出願人

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

ソニー株式会社
SONY　CORPORATION
〒141-0001 日本国東京都品川区北品川６丁目７番３５号
7-35, Kitashinagawa 6-chome, Shinagawa-ku, TOKYO 141-0001, JAPAN

☐ この欄に記載した者は、発明者でもある。

電話番号：03-5448-2617

ファクシミリ番号：03-5448-3063

加入電信番号：J22262

国籍（国名）：日本国　JAPAN

住所（国名）：日本国　JAPAN

この欄に記載した者は、次の指定国についての出願人である：☐ すべての指定国　☑ 米国を除くすべての指定国　☐ 米国のみ　☐ 追記欄に記載した指定国

第III欄　その他の出願人又は発明者

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

石橋　義人　　ISHIBASHI Yoshihito
〒141-0001 日本国東京都品川区北品川６丁目７番３５号
ソニー株式会社内
C/O SONY CORPORATION, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, TOKYO 141-0001, JAPAN

この欄に記載した者は次に該当する：

☐ 出願人のみである。

☑ 出願人及び発明者である。

☐ 発明者のみである。（ここにレ印を付したときは、以下に記入しないこと）

国籍（国名）：日本国　JAPAN

住所（国名）：日本国　JAPAN

この欄に記載した者は、次の指定国についての出願人である：☐ すべての指定国　☐ 米国を除くすべての指定国　☑ 米国のみ　☐ 追記欄に記載した指定国

☐ その他の出願人又は発明者が続葉に記載されている。

第IV欄　代理人又は共通の代表者、通知のあて名

次に記載された者は、国際機関において出願人のために行動する：☑ 代理人　☐ 共通の代表者

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

8274　弁理士　田　辺　恵　基　　TANABE Shigemoto
〒150-0001 日本国東京都渋谷区神宮前1丁目11番11-508号
グリーンファンタジアビル５階
Green-Fantasia Building 5th Floor, 11-11-508, Jingumae 1-chome, Shibuya-ku, TOKYO 150-0001, JAPAN

電話番号：03-3470-6591

ファクシミリ番号：03-3470-6506

加入電信番号：

☐ 通知のためのあて名：代理人又は共通の代表者が選任されておらず、上記枠内に特に通知が送付されるあて名を記載している場合は、レ印を付す。

第Ⅴ欄　国の指定

規則 4.9(a)の規定に基づき次の指定を行う（該当する□にレ印を付すこと；　少なくとも1つの□にレ印を付すこと）。

広域特許

☐ ＡＰ　ＡＲＩＰＯ特許：ＧＨ ガーナ Ghana, ＧＭ ガンビア Gambia, ＫＥ ケニア Kenya, ＬＳ レソト Lesotho, ＭＷ マラウイ Malawi, ＳＤ スーダン Sudan, ＳＬ シエラ・レオーネ Sierra Leone, ＳＺ スワジランド Swaziland, ＴＺ タンザニア United Republic of Tanzania, ＵＧ ウガンダ Uganda, ＺＷ ジンバブエ Zimbabwe, 及びハラレプロトコルと特許協力条約の締約国である他の国

☐ ＥＡ　ユーラシア特許：ＡＭ アルメニア Armenia, ＡＺ アゼルバイジャン Azerbaijan, ＢＹ ベラルーシ Belarus, ＫＧ キルギス Kyrgyzstan, ＫＺ カザフスタン Kazakhstan, ＭＤ モルドヴァ Republic of Moldova, ＲＵ ロシア Russian Federation, ＴＪ タジキスタン Tajikistan, ＴＭ トルクメニスタン Turkmenistan, 及びユーラシア特許条約と特許協力条約の締約国である他の国

☑ ＥＰ　ヨーロッパ特許：~~ＡＴ オーストリア Austria, ＢＥ ベルギー Belgium, ＣＨ and ＬＩ スイス及びリヒテンシュタイン Switzerland and Liechtenstein, ＣＹ キプロス Cyprus, ＤＥ ドイツ Germany, ＤＫ デンマーク Denmark, ＥＳ スペイン Spain, ＦＩ フィンランド Finland, ＦＲ フランス France, ＧＢ 英国 United Kingdom, ＧＲ ギリシャ Greece, ＩＥ アイルランド Ireland, ＩＴ イタリア Italy, ＬＵ ルクセンブルグ Luxembourg, ＭＣ モナコ Monaco, ＮＬ オランダ Netherlands, ＰＴ ポルトガル Portugal, ＳＥ スウェーデン Sweden~~, 及びヨーロッパ特許条約と特許協力条約の締約国である他の国

☐ ＯＡ　ＯＡＰＩ特許：ＢＦ ブルキナ・ファソ Burkina Faso, ＢＪ ベナン Benin, ＣＦ 中央アフリカ Central African Republic, ＣＧ コンゴー Congo, ＣＩ コートジボアール Côted'Ivoire, ＣＭ カメルーン Cameroon, ＧＡ ガボン Gabon, ＧＮ ギニア Guinea, ＧＷ ギニア・ビサオ Guinea-Bissau, ＭＬ マリ Mali, ＭＲ モーリタニア Mauritania, ＮＥ ニジェール Niger, ＳＮ セネガル Senegal, ＴＤ チャード Chad, ＴＧ トーゴー Togo, 及びアフリカ知的所有権機構のメンバー国と特許協力条約の締約国である他の国（他の種類の保護又は取扱いを求める場合には点線上に記載する）.....

国内特許（他の種類の保護又は取扱いを求める場合には点線上に記載する）

☐ ＡＥ アラブ首長国連邦 United Arab Emirates
☐ ＡＬ アルバニア Albania.....
☐ ＡＭ アルメニア Armenia.....
☐ ＡＴ オーストリア Austria.....
☐ ＡＵ オーストラリア Australia.....
☐ ＡＺ アゼルバイジャン Azerbaijan
☐ ＢＡ ボスニア・ヘルツェゴヴィナ Bosnia and Herzegovina
.....
☐ ＢＢ バルバドス Barbados
☐ ＢＧ ブルガリア Bulgaria.....
☐ ＢＲ ブラジル Brazil.....
☐ ＢＹ ベラルーシ Belarus.....
☐ ＣＡ カナダ Canada
☐ ＣＨ and ＬＩ スイス及びリヒテンシュタイン Switzerland and Liechtenstein
☑ ＣＮ 中国 China.....
☐ ＣＲ コスタリカ Costa Rica.....
☐ ＣＵ キューバ Cuba.....
☐ ＣＺ チェッコ Czech Republic.....
☐ ＤＥ ドイツ Germany.....
☐ ＤＫ デンマーク Denmark.....
☐ ＤＭ ドミニカ Dominica
☐ ＥＥ エストニア Estonia.....
☐ ＥＳ スペイン Spain.....
☐ ＦＩ フィンランド Finland.....
☐ ＧＢ 英国 United Kingdom
☐ ＧＤ グレナダ Grenada
☐ ＧＥ グルジア Georgia.....
☐ ＧＨ ガーナ Ghana.....
☐ ＧＭ ガンビア Gambia
☐ ＨＲ クロアチア Croatia.....
☐ ＨＵ ハンガリー Hungary.....
☐ ＩＤ インドネシア Indonesia
☐ ＩＬ イスラエル Israel.....
☐ ＩＮ インド India.....
☐ ＩＳ アイスランド Iceland
☐ ＪＰ 日本 Japan.....
☐ ＫＥ ケニア Kenya.....
☐ ＫＧ キルギス Kyrgyzstan.....
☐ ＫＰ 北朝鮮 Democratic People's Republic of Korea.....
☑ ＫＲ 韓国 Republic of Korea.....
☐ ＫＺ カザフスタン Kazakhstan.....
☐ ＬＣ セント・ルシア Saint Lucia
☐ ＬＫ スリ・ランカ Sri Lanka
☐ ＬＲ リベリア Liberia
☐ ＬＳ レソト Lesotho.....
☐ ＬＴ リトアニア Lithuania
☐ ＬＵ ルクセンブルグ Luxembourg
☐ ＬＶ ラトヴィア Latvia
☐ ＭＡ モロッコ Morocco.....
☐ ＭＤ モルドヴァ Republic of Moldova.....
☐ ＭＧ マダガスカル Madagascar.....
☐ ＭＫ マケドニア旧ユーゴースラヴィア共和国 The former Yugoslav Republic of Macedonia
.....
☐ ＭＮ モンゴル Mongolia
☐ ＭＷ マラウイ Malawi.....
☐ ＭＸ メキシコ Mexico.....
☐ ＮＯ ノールウェー Norway
☐ ＮＺ ニュー・ジーランド New Zealand.....
☐ ＰＬ ポーランド Poland.....
☐ ＰＴ ポルトガル Portugal.....
☐ ＲＯ ルーマニア Romania
☐ ＲＵ ロシア Russian Federation.....
☐ ＳＤ スーダン Sudan
☐ ＳＥ スウェーデン Sweden
☑ ＳＧ シンガポール Singapore
☐ ＳＩ スロヴェニア Slovenia.....
☐ ＳＫ スロヴァキア Slovakia.....
☐ ＳＬ シエラ・レオーネ Sierra Leone.....
☐ ＴＪ タジキスタン Tajikistan.....
☐ ＴＭ トルクメニスタン Turkmenistan.....
☐ ＴＲ トルコ Turkey.....
☐ ＴＴ トリニダッド・トバゴ Trinidad and Tobago.....
☐ ＴＺ タンザニア United Republic of Tanzania
☐ ＵＡ ウクライナ Ukraine.....
☐ ＵＧ ウガンダ Uganda.....
☑ ＵＳ 米国 United States of America.....
.....
☐ ＵＺ ウズベキスタン Uzbekistan.....
☐ ＶＮ ヴィエトナム Viet Nam.....
☐ ＹＵ ユーゴースラヴィア Yugoslavia.....
☐ ＺＡ 南アフリカ共和国 South Africa.....
☐ ＺＷ ジンバブエ Zimbabwe.....

下の□は、この様式の施行後に特許協力条約の締約国となった国を指定するためのものである

☐ .....
☐ .....
☐ .....

指定の確認の宣言：出願人は、上記の指定に加えて、規則 4.9(b)の規定に基づき、特許協力条約の下で認められる他の全ての国の指定を行う。ただし、この宣言から除く旨の表示を追記欄にした国は、指定から除かれる。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。（指定の確認（料金を含む）は、優先日から15月以内に受理官庁へ提出しなければならない。）

第VI欄　優先権主張

☐ 他の優先権の主張（先の出願）が追記欄に記載されている

先の出願日 (日. 月. 年)	先の出願番号	先の出願		
		国内出願 ： 国 名	広域出願 ： *広域官庁名	国際出願 ： 受理官庁名
(1) 12.04.99	平成１１年特許願 第１０３９９２号	日本国 JAPAN		
(2)				
(3)				

☑ 上記（ ）の番号の先の出願（ただし、本国際出願が提出される受理官庁に対して提出されたものに限る）のうち、次の（ ）の番号のものについては、出願書類の認証謄本を作成し国際事務局へ送付することを、受理官庁（日本国特許庁の長官）に対して請求している。 ： (1)

*先の出願が、ＡＲＩＰＯの特許出願である場合には、その先の出願を行った工業所有権の保護のためのパリ条約同盟国の少なくとも１ヶ国を追記欄に表示しなければならない（規則４．１０(b)(ii)）。追記欄を参照。

第VII欄　国際調査機関

国際調査機関（ＩＳＡ）の選択

ＩＳＡ／ＪＰ

先の調査結果の利用請求：当該調査の照会（先の調査が、国際調査機関によって既に実施又は請求されている場合）

出願日（日. 月. 年）　出願番号　国名（又は広域官庁）

第VIII欄　照合欄：出願の言語

この国際出願の用紙の枚数は次のとおりである。

願書	3 枚
明細書（配列表を除く）	71 枚
請求の範囲	5 枚
要約書	1 枚
図面	50 枚
明細書の配列表	0 枚
合計	130 枚

この国際出願には、以下にチェックした書類が添付されている。

1. ☑ 手数料計算用紙
   ☑ 納付する手数料に相当する特許印紙を貼付した書面
   ☑ 国際事務局の口座への振込みを証明する書面
2. ☐ 別個の記名押印された委任状
3. ☐ 包括委任状の写し
4. ☐ 記名押印（署名）の説明書
5. ☐ 優先権書類（上記第VI欄の（ ）の番号を記載する）：
6. ☐ 国際出願の翻訳文（翻訳に使用した言語名を記載する）：
7. ☐ 寄託した微生物又は他の生物材料に関する書面
8. ☐ ヌクレオチド又はアミノ酸配列表（フレキシブルディスク）
9. ☐ その他（書類名を詳細に記載する）：

要約書とともに提示する図面：13

本国際出願の使用言語名：日本語

第IX欄　提出者の記名押印

各人の氏名（名称）を記載し、その次に押印する。

田辺恵基

受理官庁記入欄

1. 国際出願として提出された書類の実際の受理の日

3. 国際出願として提出された書類を補充する書類又は図面であって
   その後期間内に提出されたものの実際の受理の日（訂正日）

4. 特許協力条約第１１条(2)に基づく必要な補充の期間内の受理の日

5. 出願人により特定された国際調査機関　ＩＳＡ／ＪＰ

6. ☐ 調査手数料未払いにつき、国際調査機関に調査用写しを送付していない

2. 図面
   ☐ 受理された
   ☐ 不足図面がある

国際事務局記入欄

記録原本の受理の日

この用紙は、国際出願の一部を構成せず、国際出願の用紙の枚数に[redacted]しない。

P C T

手 数 料 計 算 用 紙

願 書 附 属 書

受理官庁記入欄

国際出願番号

受理官庁の日付印

出願人又は代理人の書類記号

S00P0777WO00

出願人

ソニー株式会社　SONY CORPORATION

所定の手数料の計算

1．及び2．特許協力条約に基づく国際出願等に関する法律（国内法）第18条第1項第1号の規定による手数料 *(注1)*
（送付手数料［T］及び調査手数料［S］の合計）

95,000 円 | T+S

3．国際手数料 *(注2)*

基本手数料

国際出願に含まれる用紙の枚数 130 枚

最初の30枚まで ・・・・・・・・・・・・・・・・ 46,000 円 | b1

100 （30枚を越える用紙の枚数） × 1,100 （用紙1枚の手数料） = 110,000 円 | b2

b1及びb2に記入した金額を加算し、合計額をBに記入 156,000 円 | B

指定手数料

国際出願に含まれる指定数 *(注3)* 5

5 （支払うべき指定手数料の数 *(上限は8)* *(注4)*） × 9,900 （1指定当たりの手数料） = 49,500 円 | D

B及びDに記入した金額を加算し、合計額をIに記入・・・・・・・ 205,500 円 | I

4．納付すべき手数料の合計

T+S及びIに記入した金額を加算し、合計額を合計に記入

300,500 円

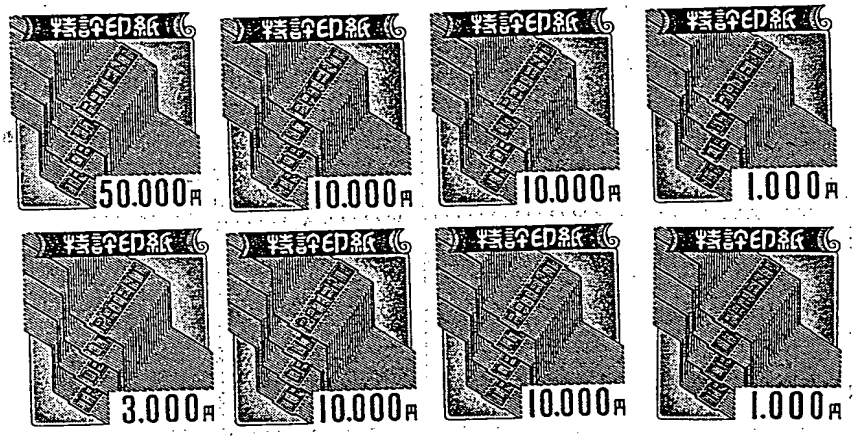
合　計

(注1) 送付手数料及び調査手数料については、合計金額を特許印紙をもって納付しなければならない。

(注2) 国際手数料については、受理官庁である日本国特許庁の長官が告示する国際事務局の口座への振込みを証明する書面を提出することにより納付しなければならない。

(注3) 願書第V欄でレ印を付した□の数。

(注4) 指定数を記入する。 ただし、8指定以上は一律8とする。



送付手数料（18,000円）
調査手数料（77,000円）

振込金(兼消費税等込手数料)受取書

ご依頼日 00年4月07日

先方銀行
漢字 ⬇ 漢字で左づめでご記入ください: 東京三菱
○印をおつけください。 銀○行 信○金 信○組 農○協 労○金 その○他
⬇ 漢字で左づめでご記入ください: 内幸町

お受取人
カタカナ (カタカナで姓と名の間はひとマスあけてください): ワイポ゜ピ゜ーシィーテ
濁点(゛)と半濁点(゜)も一字でご記入ください: イー
預金種目 ○印をおつけください。 普○通 当○座 貯○蓄 その○他
口座番号 右づめでご記入ください: 0473286
振込方法 ○印をおつけください。 電○信 文○書
金額 205,500 (十億 億 千万 百万 拾万 万 千 百 拾 円)
手数料 735
おなまえ: WIPO-PCT 様
おところ: おでんわ (03)3506-3856

ご依頼人
カタカナ (カタカナで姓と名の間はひとマスあけてください): タナヘ゛ シケ゛モト
濁点(゛)と半濁点(゜)も一字でご記入ください:
(連絡先)おでんわ 市外局番 市内局番 番号: 03-3470-6570
おなまえ: 田辺恵基 様
おところ: 渋谷区神宮前1-11-11-508 グリーンファンタジアビル5階

受取人等はカナ文字で送信しますので、フリガナは正しくていねいにご記入ください。
振込依頼書にご記入相違等の不備がありますと照会等のため振込が遅延することがあります。
午後2時以降のご用命の場合は、当日中に入金できないこともございますので、あらかじめご了承ください。
万一、通信機器・回線等の障害が生じた場合、振込が遅延したことによる補償はできませんのでご了承ください。

当行をご利用くださいましてありがとうございます。
今後ともよろしくお願い申しあげます。

翌日発信扱

当行本支店への振込のために受入れた下記の小切手等が不渡りとなったときは、その金額の振込を取消し、その小切手等は権利保全の手続きをしないで当店において返却します。

未決済小切手等

株式会社 国民銀行
原宿支店

収入印紙
振込金+手数料
3万円以上貼付
17号文書
(払戻請求書による受付書としたものは非課税)

(為104)

基本手数料 (156,000円)
指定手数料 (49,500円)
計 205,500 円

控

PCT
10.4.00
受領印

優先権証明願（ＰＣＴ）

特許庁長官　　近藤　隆彦　殿

１．出願番号　　平成１１年特許願第１０３９９２号

２．請求人

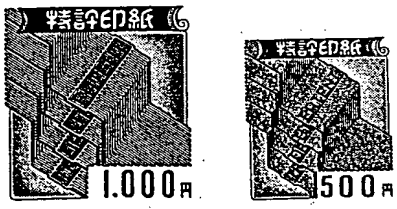
識別番号　　１０００８２７４０

住　　所　　東京都渋谷区神宮前１丁目１１番１１－５０８号
グリーンファンタジアビル５階

氏　　名　　弁理士　田辺　恵基

電話番号　　03-3470-6591

３．出願国名　　ＰＣＴ



（１，５００円）

委　任　状

私は弁理士　田 辺 恵 基 識別番号 100082740　を代理人と定めて下記事項を委任する

1. 優先権取得に関する一切の件
（特願平11-103992号）

2. 上記事件につき、出願の分割、出願の変更、放棄若しくは取下げ、特許権の存続期間の延長登録の出願の取下げ、請求、申請若しくは申立ての取下げ、特許法第４１条第１項若しくは実用新案法第８条第１項の優先権の主張若しくはその取下げ、拒絶査定に対する審判の請求、実用新案登録出願若しくは実用新案登録についての実用新案技術評価の請求、又は復代理人の選任若しくは解任をするの件

以上

平成 12 年 4 月 7 日

東京都品川区北品川６丁目７番35号

ソニー株式会社

代表取締役 出 井 伸 之

EP US

特　許　協　力　条　約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　S00P0777WO00	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０２２９０	国際出願日 （日.月.年）　０７．０４．００	優先日 （日.月.年）　１２．０４．９９
出願人（氏名又は名称） ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　2　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

a．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　１３　図とする。
☒ 出願人が示したとおりである。　　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０２２９０

A　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int. Cl' G06F17/60

B　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int. Cl' G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1926-1996年
日本国公開実用新案公報　1971-2000年
日本国実用新案登録公報　1996-2000年
日本国登録実用新案公報　1994-2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTファイル(JOIS)

C　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO,96/27155,A2(InerTrust Technologies Corp.)6.9月.1996(06.09.96)&JP,10-512074,A	1-8
Y	人文科学とコンピュータ，第36-8巻，11月.1997 河原正治「著作権処理技術の最近の動向」p.43-48	1-8

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
24.05.00	13.06.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	岩間　直純	5L	9287
	電話番号　０３－３５８１－１１０１　内線　3562		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7 G06F 17/60	A1	(11) 国際公開番号	WO00/62217
		(43) 国際公開日	2000年10月19日(19.10.00)

(21) 国際出願番号 PCT/JP00/02290

(22) 国際出願日 2000年4月7日(07.04.00)

(30) 優先権データ
特願平11/103992 1999年4月12日(12.04.99) JP

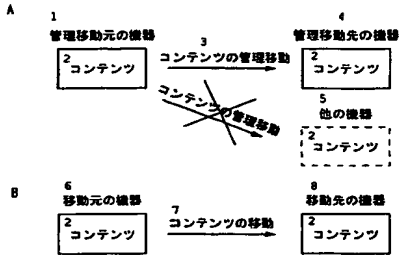
(71) 出願人（米国を除くすべての指定国について）
ソニー株式会社(SONY CORPORATION)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
石橋義人(ISHIBASHI, Yoshihito)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号
ソニー株式会社内 Tokyo, (JP)
(74) 代理人
弁理士 田辺恵基(TANABE, Shigemoto)
〒150-0001 東京都渋谷区神宮前1丁目11番11-508号
グリーンフアンタジアビル5階 Tokyo, (JP)

(81) 指定国 CN, KR, SG, US, 欧州特許 (DE, FR, GB)

添付公開書類
国際調査報告書

(54)Title: INFORMATION PROCESSING DEVICE AND METHOD, AND PROVIDING MEDIUM

(54)発明の名称 情報処理装置および方法、並びに提供媒体



A
1...DEVICE OF MANAGEMENT TRANSFER SOURCE
2...CONTENTS
3...TRANSFER CONTENTS MANAGEMENT
4...DEVICE OF MANAGEMENT TRANSFER DESTINATION
5...ANOTHER DEVICE

B
6...DEVICE OF TRANSFER SOURCE
7...TRANSFER OF CONTENTS
8...DEVICE OF TRANSFER DESTINATION

(57) Abstract

Contents can be transferred while the device which is the source of the contents holds them. The contents are transferred to a device of a management transfer destination while being held in the device of the management transfer source. The contents are used by both the device of the management transfer source and the device of the management transfer destination. This is different from ordinary transfer that the contents are not held in the device of the transfer source but used exclusively by the device of the transfer destination. During the management transfer of the contents, the device of the management transfer source cannot transfer the management of the contents to another device. The contents are held exclusively in the two devices, the device of the management transfer source and the device of the management transfer destination. This is different from duplication of the first generation that a plurality of duplicates (of the first generation) can be created from the original contents. This is also different from the one-time duplication because the management of the contents can be transferred to another device by returning them from the device of the management transfer source.

(57)要約

コンテンツの移動元の機器が、コンテンツを保持しつつ、コンテンツを移動させることができるようにする。

管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。つまり、移動元の機器にコンテンツが保持されず、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。コンテンツの管理移動が行われている間、管理移動元の機器は、他の機器にコンテンツを管理移動することができない。管理移動元の機器と管理移動先の機器の２機においてのみコンテンツが保持される。つまり、オリジナルのコンテンツから、複数の複製（第１世代）を作成することができる、第１世代の複製とも異なる。管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、１回だけの複製とも異なる。

明　細　書

情報処理装置および方法、並びに提供媒体

技術分野

本発明は、情報処理装置および方法、並び提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

背景技術

音楽などの情報（以下、コンテンツと称する）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、情報処理装置でコンテンツを復号して、利用するシステムがある。

また、コンテンツを利用することができる情報処理装置が複数存在する場合、ユーザは、提供されてコンテンツを移動させ、コンテンツが移動された情報処理装置において、コンテンツを利用することもできる。

しかしながら、この場合、コンテンツは移動元の情報処理装置が保持されず、ユーザが、移動元の情報処理装置において、そのコンテンツを利用できない課題があった。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、コンテンツが移動元の情報処理装置にも保持され、他の情報処理装置にコンテンツを移動させることができるようにするものである。

かかる課題を解決するため本発明においては、情報処理装置において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置において、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する

記憶手段と、記憶手段により記憶されている利用情報に含まれる前記使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報を他の情報処理装置に供給する供給手段と、供給手段により、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更する第１の変更手段と、記憶手段により記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行われていることを示しており、情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号を送信する送信手段と、他の情報処理装置から、送信手段により送信された制御信号に対する応答信号を受信したとき、移動状態情報の内容を、価値情報の移動が行われていないことを示すものに変更する第２の変更手段とを具備する。

また本発明においては、情報処理方法において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置の情報処理方法において、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、記憶ステップで記憶された利用情報に含まれる使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報を他の情報処理装置に供給する供給ステップと、供給ステップで、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更する第１の変更ステップと、記憶ステップで記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行われていることを示しており、情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号を送信する送信ステップと、他の情報処理装置から、送信ステップで送信された制御信号に対する応答信号を受信したとき、移動状態情報の内容を、価値情報の移動が行われていないこ

とを示すものに変更する第２の変更ステップを具備する。

さらに本発明においては、提供媒体において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置に、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、記憶ステップで記憶された利用情報に含まれる使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報を他の情報処理装置に供給する供給ステップと、供給ステップで、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更する第１の変更ステップと、記憶ステップで記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行われていることを示しており、他の情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号を送信する送信ステップと、他の情報処理装置から、送信ステップで送信された制御信号に対する応答信号を受信したとき、移動状態情報の内容を、価値情報の移動が行われていないことを示すものに変更する第２の変更ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供。

さらに本発明においては、情報処理装置、情報処理方法、および提供媒体において、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報が記憶され、記憶された利用情報に含まれる使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報が他の情報処理装置に供給され、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容が、価値情報の移動が行われていることを示すものに変更され、記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行わ

れていることを示しており、他の情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号が送信され、他の情報処理装置から、制御信号に対する応答信号が受信されたとき、移動状態情報の内容が、価値情報の移動が行われていないことを示すものに変更される。

さらに本発明においては、情報処理装置において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置において、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信する受信手段と、受信手段により受信された移動情報を記憶する記憶手段と、他の情報処理装置から、所定の制御信号を受信したとき、記憶手段に記憶されている移動情報を削除する削除手段と、削除手段により、移動情報が削除されたとき、所定の応答信号を送信する送信手段を具備する。

さらに本発明においては、情報処理方法において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置の情報処理方法において、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、受信ステップで受信された移動情報を記憶する記憶ステップと、他の情報処理装置から、所定の制御信号を受信したとき、記憶ステップで記憶された移動情報を削除する削除ステップと、削除ステップで、移動情報が削除されたとき、所定の応答信号を送信する送信ステップを具備する。

さらに本発明においては、提供媒体において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置に、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、受信ステップで受信された移動情報を記憶する記憶ステップと、他の情報処理装置から、所定の制御信号を受信したとき、記憶ステップで記憶された移動情報を削除する削除ステップと、削除ステップで、移動情報が削除されたとき、所定の応答信号を送信する送信ステップとを具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴と

する。

さらに本発明においては、情報処理装置、情報処理方法、および提供媒体において、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報が受信され、受信された価値情報が記憶され、他の情報処理装置から、所定の制御信号を受信したとき、記憶された移動情報が削除され、移動情報が削除されたとき、所定の応答信号が送信される。

図面の簡単な説明

図１は、ＥＭＤシステムを説明する系統図である。

図２は、ＥＭＤシステムにおける、主な情報の流れを説明する系統図である。

図３は、ＥＭＤサービスセンタ１の機能的構成を示すブロック図である。

図４は、ＥＭＤサービスセンタ１の配送用鍵Ｋｄの送信を説明する略線図である。

図５は、ＥＭＤサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の略線図である。

図６は、ＥＭＤサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の略線図である。

図７は、ＥＭＤサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の略線図である。

図８は、ＥＭＤサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の図表である。

図９は、システム登録情報を説明する図表である。

図１０は、利用ポイント情報を説明する図表である。

図１１は、コンテンツプロバイダ２の機能的構成例を示すブロック図である。

図１２は、ＵＣＰを説明する図表である。

図１３は、コンテンツの管理移動を説明する略線図である。

図１４は、第１世代複製を説明する略線図である。

図１５は、サービスコードおよびコンディションコードのコード値の例を示す図表である。

図１６は、ＵＣＰの利用条件として設定されたコード値の例を示す図表である。

図１７は、コンテンツプロバイダセキュアコンテナの例を示す略線図である。

図１８は、コンテンツプロバイダ２の証明書の例を示す略線図である。

図１９は、サービスプロバイダ３の機能の構成を示すブロック図である。

図２０は、ＰＴの例を示す図表である。

図２１は、ＰＴの価格条件として設定されたコード値の例を示す図表である。

図２２は、他のＰＴの例を示す図表である。

図２３は、他のＰＴの価格条件として設定されたコード値の例を示す図表である。

図２４は、サービスプロバイダセキュアコンテナの例を示す略線図である。

図２５は、サービスプロバイダ３の証明書の例を示す略線図である。

図２６は、ユーザホームネットワーク５のレシーバ５１の機能的構成例を示すブロック図である。

図２７は、レシーバ５１のＳＡＭ６２の証明書の例を示す略線図である。

図２８は、ＵＣＳの例を示す図表である。

図２９は、レシーバ５１の外部記憶部６３の利用情報記憶部６３Ａの内部を説明する略線図である。

図３０は、課金情報の例を示す図表である。

図３１は、レシーバ５１の記憶モジュール７３に記憶されている情報を示す図表である。

図３２は、基準情報５１を説明する図表である。

図３３は、基準情報５１の利用ポイント情報の例を示す図表である。

図３４は、登録リストの例を示す図表である。

図３５は、ユーザホームネットワーク５のレシーバ２０１の機能的構成例を示

すブロック図である。

図３６は、レシーバ２０１の外部記憶部２１３の移動情報記憶部２１３Ａの内部を説明する略線図である。

図３７は、レシーバ２０１の記憶モジュール２２３に記憶されている情報を示す図表である。

図３８は、コンテンツの利用処理を説明するフローチャートである。

図３９は、ＥＭＤサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信する処理を説明するフローチャートである。

図４０は、コンテンツプロバイダ２とＥＭＤサービスセンタ１との相互認証の動作を説明するフローチャートである。

図４１は、コンテンツプロバイダ２とＥＭＤサービスセンタ１との相互認証の他の動作を説明するフローチャートである。

図４２は、コンテンツプロバイダ２とＥＭＤサービスセンタ１との相互認証の他の動作を説明するフローチャートである。

図４３は、コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図４４は、サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図４５は、レシーバ５１がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

図４６は、レシーバ５１がコンテンツを再生する処理を説明するフローチャートである。

図４７は、課金を決済する処理を説明するフローチャートである。

図４８は、コンテンツを管理移動する処理を説明するフローチャートである。

図４９は、コンテンツの管理移動を終了する処理を説明するフローチャートである。

発明を実施するための最良の形態

以下に本発明の実施の形態を説明する。

（１）情報配信システム

図１は、本発明を適用したＥＭＤ（Ｅｌｅｃｔｒｏｎｉｃ　Ｍｕｓｉｃ　Ｄｉｓｔｒｉｂｕｔｉｏｎ：電子音楽配信）システムを説明する図である。ＥＭＤシステムは、各装置を管理するＥＭＤサービスセンタ１、コンテンツを提供するコンテンツプロバイダ２（この例の場合、２つのコンテンツプロバイダ２－１，２－２（以下、個々に区別する必要がない場合、単に、コンテンツプロバイダ２と記述する。他の装置についても同様である）が設けられている）、コンテンツに対応するサービスを提供するサービスプロバイダ３（この例の場合、２つのサービスプロバイダ３－１，３－２が設けられている）、およびコンテンツが利用されるユーザネットワーク５から構成されている。

ＥＭＤシステムにおけるコンテンツ（Ｃｏｎｔｅｎｔ）とは、情報そのものが価値を有するデジタルデータで、この例の場合、１つのコンテンツは、１曲分の音楽データに相当する。またコンテンツは、１つのコンテンツを１つの単位（シングル）として、または複数のコンテンツを１つの単位（アルバム）としてユーザに提供される。ユーザは、コンテンツを購入し（実際は、コンテンツを利用する権利を購入し）、コンテンツを利用する。尚、コンテンツは、音楽データだけでなく、映像データ、ゲームプログラム、コンピュータプログラム、著作データなどの場合も有りうる。

ＥＭＤサービスセンタ１は、ＥＭＤシステムにおける主な情報の流れを示す図２に示すように、ユーザホームネットワーク５、およびコンテンツプロバイダ２に、コンテンツを利用するために必要な配送用鍵Ｋｄを送信する。ＥＭＤサービスセンタ１はまた、ユーザホームネットワーク５の機器から、課金情報等を受信して、料金を精算する処理などを実行する。

コンテンツプロバイダ２－１，２－２は、図２に示すように、提供するコンテンツ（コンテンツ鍵Ｋｃｏで暗号化されている）、そのコンテンツを復号するた

めに必要なコンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）、およびコンテンツの利用内容などを示す取扱方針（以下、ＵＣＰ（Ｕｓａｇｅ　Ｃｏｎｔｒｏｌ　Ｐｏｌｉｃｙ）と記述する）を保持し、それらを、コンテンツプロバイダセキュアコンテナ（後述）と称する形態で、サービスプロバイダ３に供給する。

サービスプロバイダ３－１，３－２は、コンテンツプロバイダ２から供給されるＵＣＰに対応して、１つまたは複数の価格情報（以下、ＰＴ（Ｐｒｉｃｅ　Ｔａｇ）と記述する）を作成し、それを保持する。サービスプロバイダ２は、作成したＰＴを、コンテンツプロバイダ２から供給されたコンテンツ（コンテンツ鍵Ｋｃｏで暗号化されている）、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）、およびＵＣＰとともに、サービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク４を介して、ユーザホームネットワーク５に送信する。

ユーザホームネットワーク５は、供給されたＵＣＰおよびＰＴに基づいて、図２に示すように、使用許諾条件情報（以下、ＵＣＳ（Ｕｓａｇｅ　Ｃｏｎｔｒｏｌ　Ｓｔａｔｕｓ）と称する）を作成し、作成したＵＣＳに基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク５はまた、ＵＣＳを作成するタイミングで課金情報を作成し、例えば、配送用鍵Ｋｄの供給を受けるタイミングで、対応するＵＣＰおよびＰＴなどとともにＥＭＤサービスセンタ１に送信する。なお、ユーザホームネットワーク５は、ＵＣＰおよびＰＴをＥＭＤサービスセンタ１に送信しないようにすることもできる。

この例の場合、ユーザホームネットワーク５は、ＨＤＤ５２に接続され、ＳＡＭ（Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｍｏｄｕｌｅ）６２を有するレシーバ５１、およびＨＤＤ２０２に接続され、ＳＡＭ２１２を有するレシーバ２０１から構成されている。レシーバ５１とレシーバ２０１は、ＩＥＥＥ１３９４等で接続されている。

（２）ＥＭＤサービスセンタ

図３は、ＥＭＤサービスセンタ１の機能的構成を示すブロック図である。サービスプロバイダ管理部１１は、サービスプロバイダ３に利益分配の情報を供給する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信したり、利益分配の情報を供給する。

著作権管理部１３は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、ＪＡＳＲＡＣ（Ｊａｐａｎｅｓｅ Ｓｏｃｉｅｔｙ ｆｏｒ Ｒｉｇｈｔｓ ｏｆ Ａｕｔｈｏｒｓ，Ｃｏｍｐｏｓｅｒｓ ａｎｄ Ｐｕｂｌｉｓｈｅｒｓ：日本音楽著作権協会）に送信する。

鍵サーバ１４は、配送用鍵Ｋｄを記憶しており、それを、コンテンツプロバイダ管理部１２を介してコンテンツプロバイダ２に供給したり、ユーザ管理部１８等を介してユーザホームネットワーク５に供給する。

ユーザホームネットワーク５の機器（例えば、レシーバ５１またはレシーバ２０１）およびコンテンツプロバイダ２に供給される、ＥＭＤサービスセンタ１からの配送用鍵Ｋｄについて、図４乃至図７を参照して説明する。

図４は、コンテンツプロバイダ２がコンテンツの提供を開始し、ユーザホームネットワーク５を構成するレシーバ５１がコンテンツの利用を開始する、１９９８年１月における、ＥＭＤサービスセンタ１が有する配送用鍵Ｋｄ、コンテンツプロバイダ２が有する配送用鍵Ｋｄ、およびレシーバ５１が有する配送用鍵Ｋｄを示す図である。

図４の例において、配送用鍵Ｋｄは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である”ａａａａａａａａ”の値を有するバージョン１である配送用鍵Ｋｄは、１９９８年１月１日から１９９８年１月３１日まで使用可能（すなわち、１９９８年１月１日から１９９８年１月３１日の期間にサービスプロバイダ３を介してユーザホームネットワーク５に配布されるコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン１である配送

用鍵Ｋｄで暗号化されている）であり、所定のビット数の乱数である”ｂｂｂｂｂｂｂｂ”の値を有するバージョン２である配送用鍵Ｋｄは、１９９８年２月１日から１９９８年２月２８日まで使用可能（すなわち、その期間にサービスプロバイダ３を介してユーザホームネットワーク５に配布されるコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン２である配送用鍵Ｋｄで暗号化されている）である。同様に、バージョン３である配送用鍵Ｋｄは、１９９８年３月中に使用可能であり、バージョン４である配送用鍵Ｋｄは、１９９８年４月中に使用可能であり、バージョン５である配送用鍵Ｋｄは、１９９８年５月中に使用可能であり、バージョン６である配送用鍵Ｋｄは、１９９８年６月中に使用可能である。

コンテンツプロバイダ２がコンテンツの提供を開始するに先立ち、ＥＭＤサービスセンタ１は、コンテンツプロバイダ２に、１９９８年１月から１９９８年６月まで利用可能な、バージョン１乃至バージョン６の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、記憶する。６ヶ月分の配送用鍵Ｋｄを記憶するのは、コンテンツプロバイダ２が、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

また、レシーバ５１がコンテンツの利用を開始するに先立ち、ＥＭＤサービスセンタ１は、レシーバ５１に、１９９８年１月から１９９８年３月まで、利用可能なバージョン１乃至バージョン３である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、記憶する。３ヶ月分の配送用鍵Ｋｄを記憶するのは、レシーバ５１が、ＥＭＤサービスセンタ１に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、ＥＭＤサービスセンタ１への接続の頻度を低くし、ユーザホームネットワーク５の負荷を低減するためである。

１９９８年１月１日から１９９８年１月３１日の期間には、バージョン１であ

る配送用鍵Ｋｄが、ＥＭＤサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

１９９８年２月１日における、ＥＭＤサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図５で説明する。ＥＭＤサービスセンタ１は、コンテンツプロバイダ２に、１９９８年２月から１９９８年７月まで利用可能な、バージョン２乃至バージョン７の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、レシーバ５１に、１９９８年２月から１９９８年４月まで、利用可能なバージョン２乃至バージョン４である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、バージョン１である配送用鍵Ｋｄをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Ｋｄを利用できるようにするためである。

１９９８年２月１日から１９９８年２月２８日の期間には、バージョン２である配送用鍵Ｋｄが、ＥＭＤサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

１９９８年３月１日における、ＥＭＤサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図６で説明する。ＥＭＤサービスセンタ１は、コンテンツプロバイダ２に、１９９８年３月から１９９８年８月まで利用可能な、バージョン３乃至バージョン８の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、レシーバ５１に、１９９８年３月から１９９８年５月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋ

ｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、バージョン１である配送用鍵Ｋｄおよびバージョン２である配送用鍵Ｋｄをそのまま記憶する。

１９９８年３月１日から１９９８年３月３１日の期間には、バージョン３である配送用鍵Ｋｄが、ＥＭＤサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

１９９８年４月１日における、ＥＭＤサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図７で説明する。ＥＭＤサービスセンタ１は、コンテンツプロバイダ２に、１９９８年４月から１９９８年９月まで利用可能な、バージョン４乃至バージョン９の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、レシーバ５１に、１９９８年４月から１９９８年６月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、バージョン１である配送用鍵Ｋｄ、バージョン２である配送用鍵Ｋｄ、およびバージョン３である配送用鍵Ｋｄをそのまま記憶する。

１９９８年４月１日から１９９８年４月３０日の期間には、バージョン４である配送用鍵Ｋｄが、ＥＭＤサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

このように、あらかじめ先の月の配送用鍵Ｋｄを配布しておくことで、仮にユーザが１，２ヶ月まったくＥＭＤサービスセンタ１にアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、ＥＭＤサービスセンタ１にアクセスして鍵を受信することができる。

ユーザホームネットワーク５の、ＥＭＤシステムに正式登録された機器、およびコンテンツプロバイダ２には、以上のように、３ヶ月分の配送用鍵Ｋｄが配布

されるが、ＥＭＤシステムに正式登録されておらず、仮登録（詳細は後述する）されている状態の、ユーザホームネットワーク５の機器には、３ヶ月分の配送用鍵Ｋｄに代わり、図８に示すような、１ヶ月分の配送用鍵Ｋｄが配布される。この例においては、ユーザホームネットワーク５の機器をＥＭＤシステムに正式登録するために、与信処理など、約１ヶ月程度の時間を有する登録手続が必要となる。そこで、登録申請から正式登録されるまでの間（約１ヶ月間）においても、コンテンツの利用が可能となるように、正式登録されていない機器（仮登録されている機器）には、１ヶ月間において利用可能な配送用鍵Ｋｄが配布される。

図３に戻り、経歴データ管理部１５は、ユーザ管理部１８から出力される、課金情報、そのコンテンツに対応するＰＴ、およびそのコンテンツに対応するＵＣＰなどを記憶する。

利益分配部１６は、経歴データ管理部１５から供給された各種情報に基づき、ＥＭＤサービスセンタ１、コンテンツプロバイダ２－１，２－２、およびサービスプロバイダ３－１，３－２の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部１１、コンテンツプロバイダ管理部１２、出納部２０、および著作権管理部１３に出力する。利益配分部１６はまた、算出した利益に応じてコンテンツプロバイダ２－１，２－２およびサービスプロバイダ３－１，３－２のそれぞれに対する利用ポイント（利益が大きければ大きいほど、すなわち、ユーザが利用すればするほど、大きい値となるポイント）を算出し、ユーザ管理部１８に出力する。なお、以下において、コンテンツプロバイダ２における利用ポイントをコンテンツ利用ポイントと称し、サービスプロバイダ３における利用ポイントをサービス利用ポイントと称する。

相互認証部１７は、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の機器と相互認証を実行する。

ユーザ管理部１８は、ユーザホームネットワーク５の機器に関する情報（以下、システム登録情報と称する）を管理する。システム登録情報には、図９に示すように、「ＳＡＭのＩＤ」、「機器番号」、「決済ＩＤ」、「決済ユーザ情報」

、複数の「従属ユーザ情報」、および「利用ポイント情報」の項目に対応する所定の情報が含まれている。

「ＳＡＭのＩＤ」には、製造された、ユーザホームネットワーク５の機器のＳＡＭのＩＤが記憶される。図９のシステム登録情報の「ＳＡＭのＩＤ」には、レシーバ５１のＳＡＭ６２のＩＤおよびレシーバ２０１のＳＡＭ２１２のＩＤが設定されている。

「機器番号」には、ＳＡＭを有するユーザホームネットワーク５の機器に、予め設定された機器番号が設定されている。ユーザホームネットワーク５の機器が、ネットワーク４を介してサービスプロバイダ３と、およびＥＭＤサービスセンタ１と直接通信することができる機能を有し（通信部を有し）、かつ、例えば、ＵＣＰやＰＴの内容をユーザに出力（提示）したり、ユーザがＵＣＰの利用内容を選択することができる機能を有している（表示部および操作部を有している）場合、その機器（以下、主機器と称する）には、１００番以上の機器番号が与えられる。機器が、そのような機能を有しいない場合、その機器（以下、従機器と称する）には、９９番以下の機器番号が与えられる。この例の場合、詳細は後述するが、レシーバ５１およびレシーバ２０１の両者は、上述した機能を有しているので、それぞれには、１００番以上の機器番号（１００番）が与えられてる。そこで、図９のシステム登録情報の「機器番号」には、レシーバ５１のＳＡＭ６２のＩＤおよびレシーバ２０１のＳＡＭ２１２のＩＤに対応する「機器番号」のそれぞれには、機器番号１００番が設定されている。

「決済ＩＤ」には、ＥＭＤシステムに正式登録されたとき割り当てられる所定の決済ＩＤが記憶される。この例の場合、レシーバ５１およびレシーバ２０１は共に、正式登録され、決済ＩＤが与えられているので、図９のシステム登録情報の、ＳＡＭ６２のＩＤにおよびＳＡＭ２１２のＩＤに対応する「決済ＩＤ」のそれぞれには、その与えられた決済ＩＤが記憶されている。

「決済ユーザ情報」には、計上される課金を決済するユーザ（以下、このようなユーザを決済ユーザと称する）の、氏名、住所、電話番号、決済機関情報（例

えば、クレジットカード番号等）、生年月日、年齢、性別、ＩＤ、パスワードなどが設定される。

「決済ユーザ情報」に設定される決済ユーザの、氏名、住所、電話番号、決済機関の情報、生年月日、および性別（以下、ここに区別する必要がない場合、これらの情報をまとめて、ユーザ一般情報と称する）は、登録が申請される際にユーザから提供され、設定されるが、この例の場合、そのうち、氏名、住所、電話番号、および決済機関の情報は、それらに基づいて与信処理が行われるので、正確な情報（例えば、決済機関に登録されている情報）である必要がある。それに対して、ユーザ一般情報の生年月日、年齢、および性別は、与信処理には用いられないので、この例の場合、それらの情報は、正確である必要はなく、またユーザは、その情報を必ずしも提供する必要がない。「決済ユーザ情報」に記憶される決済ユーザの、ＩＤおよびパスワードは、ＥＭＤシステムに仮登録されるときに割り当てられ、設定される。

図９のシステム登録情報には、レシーバ５１のＳＡＭ６２のＩＤに対応する「決済ユーザ情報」には、レシーバ５１の決済ユーザである、ユーザＦの、ユーザ一般情報、ＩＤ、およびパスワードが設定され、レシーバ２０１のＳＡＭ２１２のＩＤに対応する「決済ユーザ情報」には、レシーバ２０１の決済ユーザである、ユーザＡの、ユーザ一般情報、ＩＤ、およびパスワードが設定されている。

「従属ユーザ情報」には、課金を決済しないユーザ（以下、このようなユーザを従属ユーザと称する）の、氏名、住所、電話番号、生年月日、年齢、性別、ＩＤ、パスワードなどが設定される。すなわち、「決済ユーザ情報」に設定される情報のうち、決済機関の情報以外の情報が設定される。従属ユーザに対しては与信処理が行われないので、「従属ユーザ情報」に設定される従属ユーザの、氏名、住所、電話番号、生年月日、年齢、および性別の情報は、正確なものである必要がない。例えば、氏名の場合は、ニックネームのようなものでもよい。また氏名はユーザを特定するために必要とされるが、他の情報は、ユーザは必ずしも提供する必要がない。「従属ユーザ情報」に設定される従属ユーザの、ＩＤおよび

パスワードは、仮登録または正式登録されるときに割り当てられ、設定される。

この例の場合、レシーバ５１およびレシーバ２０１の両者には、従属ユーザが登録されていないので、図９のシステム登録情報のＳＡＭ６２のＩＤに対応する「従属ユーザ情報」、およびＳＡＭ２１２のＩＤに対応する「従属ユーザ情報」には、何の情報も設定されていない。

「利用ポイント情報」には、利益分配部１６から出力された利用ポイントが設定される。この例の場合、ＳＡＭ６２およびＳＡＭ２１２に対応する「利用ポイント情報」には、それぞれの利用ポイント情報が設定されている。図１０は、レシーバ５１の利用ポイント情報の例を示している。図１０の例では、レシーバ５１のユーザＦ（決済ユーザ）に与えられている、コンテンツプロバイダ２－１のコンテンツ利用ポイントが２２２ポイントで、コンテンツプロバイダ２－２のコンテンツ利用ポイントが１２３ポイントで、サービスプロバイダ３－１のサービス利用ポイントが、３４５ポイントで、そして、サービスプロバイダ３－２のサービス利用ポイントが０ポイントであるとされている。

なお、この例において、コンテンツプロバイダ２－１およびコンテンツプロバイダ２－２のそれぞれのコンテンツ利用ポイントの合計ポイント３４５（＝１２３＋２２２）と、サービスプロバイダ３－１およびサービスプロバイダ３－２のそれぞれのサービス利用ポイントの合計ポイント３４５（＝３４５＋０）が等しくなるようになされている。

レシーバ２０１においては、現時点でコンテンツは利用されていないので、ＳＡＭ２１２のＩＤに対応する「利用ポイント情報」には、何の情報の設定されていない。

ユーザ管理部１８は、このようなシステム登録情報を管理する他、所定の処理に対応して登録リスト（後述）を作成し、配送用鍵Ｋｄとともにユーザホームネットワーク５に送信する。

図３に、再度戻り、課金請求部１９は、経歴データ管理部１５から供給された、例えば、課金情報、ＵＣＰ、およびＰＴに基づき、ユーザへの課金を算出し、

その結果を、出納部２０に供給する。出納部２０は、ユーザ、コンテンツプロバイダ２、およびサービスプロバイダ３への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部２０はまた、決算処理の結果をユーザ管理部１８に通知する。

監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、ＰＴ、およびＵＣＰの正当性（すなわち、不正をしていないか）を監査する。なお、この場合、監査部２１は、コンテンツプロバイダ２からのＵＣＰを、サービスプロバイダ３からのＰＴを、そしてユーザホームネットワーク５からの、対応するＵＣＰおよびＰＴを受け取る。

（３）コンテンツプロバイダ

図１１は、コンテンツプロバイダ２－１の機能的構成を示すブロック図である。コンテンツサーバ３１は、ユーザに供給するコンテンツを記憶し、ウォータマーク付加部３２に供給する。ウォータマーク付加部３２は、コンテンツサーバ３１から供給されたコンテンツにウォータマーク（電子透かし）を付加し、圧縮部３３に供給する。

圧縮部３３は、ウォータマーク付加部３２から供給されたコンテンツを、ＡＴＲＡＣ２（Ａｄａｐｔｉｖｅ　Ｔｒａｎｓｆｏｒｍ　Ａｃｏｕｓｔｉｃ　Ｃｏｄｉｎｇ　２）（商標）等の方式で圧縮し、暗号化部３４に供給する。暗号化部３４は、圧縮部３３で圧縮されたコンテンツを、乱数発生部３５から供給された乱数を鍵（以下、この乱数をコンテンツ鍵Ｋｃｏと称する）として、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

乱数発生部３５は、コンテンツ鍵Ｋｃｏとなる所定のビット数の乱数を暗号化部３４および暗号化部３６に供給する。暗号化部３６は、コンテンツ鍵ＫｃｏをＥＭＤサービスセンタ１から供給された配送用鍵Ｋｄを使用して、ＤＥＳなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

ＤＥＳは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして処理する暗号方式である。ＤＥＳの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。ＤＥＳのすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

まず、平文の６４ビットは、上位３２ビットのH_0、および下位３２ビットのL_0に分割される。鍵処理部から供給された４８ビットの拡大鍵K_1、および下位３２ビットのL_0を入力とし、下位３２ビットのL_0を攪拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのH_0と、Ｆ関数の出力が排他的論理和され、その結果はL_1とされる。L_0は、H_1とされる。

上位３２ビットのH_0および下位３２ビットのL_0を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのH_{16}および下位３２ビットのL_{16}が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

ポリシー記憶部３７は、コンテンツに対応して設定されるＵＣＰを記憶し、セキュアコンテナ作成部３８に出力する。図１２は、コンテンツサーバ３１に保持されているコンテンツＡに対応して設定され、ポリシー記憶部３７に記憶されているたＵＣＰＡ、Ｂを表している。ＵＣＰは、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「ＵＣＰの有効期限」、「利用条件」、「利用内容」の各項目に対応する所定の情報が含まれる。「コンテンツのＩＤ」には、ＵＣＰが対応するコンテンツのＩＤが設定される。ＵＣＰＡ（図１２Ａ）およびＵＣＰＢ（図１２Ｂ）のそれぞれの「コンテンツのＩＤ」には、コンテンツＡのＩＤが設定されている。

「コンテンツプロバイダのＩＤ」には、コンテンツの提供元のコンテンツプロバイダのＩＤが設定される。ＵＣＰＡおよびＵＣＰＢのそれぞれの「コンテンツ

プロバイダのＩＤ」には、コンテンツプロバイダ２－１のＩＤが設定されている。「ＵＣＰのＩＤ」には、各ＵＣＰに割り当てられた所定のＩＤが設定され、ＵＣＰＡの「ＵＣＰのＩＤ」には、ＵＣＰＡのＩＤが、ＵＣＰＢの「ＵＣＰのＩＤ」には、ＵＣＰＢのＩＤが、それぞれ設定されている。「ＵＣＰの有効期限」には、ＵＣＰの有効期限を示す情報が設定され、ＵＣＰＡの「ＵＣＰの有効期限」には、ＵＣＰＡの有効期限が、U.CＰＢの「ＵＣＰの有効期限」には、ＵＣＰＢの有効期限が、それぞれ設定されている。

「利用条件」には、「ユーザ条件」および「機器条件」の各項目に対応する所定の情報が設定され、「ユーザ条件」には、このＵＣＰを選択することができるユーザの条件が設定され、「機器条件」には、このＵＣＰを選択することができる機器の条件が設定されている。

ＵＣＰＡの場合、「利用条件１０」が設定され、「利用条件１０」の「ユーザ条件１０」には、利用ポイントが２００ポイント以上であることが条件であることを示す情報（”２００ポイント以上”）が設定されている。また「利用条件１０」の「機器条件１０」には、条件がないことを示す情報（”条件なし”）が設定されている。すなわち、ＵＣＰＡは、２００ポイント以上のコンテンツプロバイダ２－１のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

ＵＣＰＢの場合、「利用条件２０」が設定され、「利用条件２０」の「ユーザ条件２０」には、利用ポイントが２００ポイントより少ないことが条件であることを示す情報（”２００ポイントより少ない”）が設定されている。また「利用条件２０」の「機器条件２０」には、”条件なし”が設定されている。すなわち、ＵＣＰＢは、２００ポイントより少ないコンテンツプロバイダ２－１のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

「利用内容」には、「ＩＤ」、「形式」、「パラメータ」、および「管理移動許可情報」の各項目に対応する所定の情報が含まれる。「ＩＤ」には、「利用内容」に設定される情報に割り当てられた所定のＩＤが設定される。「形式」には、再生や複製など、コンテンツの利用形式を示す情報が設定される。「パラメー

タ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されているか否か）を示す情報（”可”または”不可”）が設定される。コンテンツの管理移動が行われると、図１３Ａに示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図１３Ｂに示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図１３Ａに示すように、他の機器にコンテンツを管理移動することができない（許可されていない）。すなわち、管理移動元の機器と管理移動先の機器の２機においてのみコンテンツが保持される。この点で、図１４Ａに示すように、オリジナルのコンテンツから、複数の複製（第１世代）を作成することができる、第１世代の複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図１４Ｂに示すように、１回だけの複製とも異なる。

図１２Ａに戻り、ＵＣＰＡには、４つの「利用内容１１」乃至「利用内容１４」が設けられており、「利用内容１１」において、その「ＩＤ１１」には、「利用内容１１」に割り当てられた所定のＩＤが設定されている。「形式１１」には、コンテンツを買い取って再生する利用形式を示す情報（”買い取り再生”）が設定され、「パラメータ１１」には、”買い取り再生”に対応する所定の情報が設定されている。「管理移動許可情報１１」には、コンテンツの管理移動が許可されていることを示す情報（”可”）が設定されている。

「利用内容１２」において、その「ＩＤ１２」には、「利用内容１２」に割り当てられた所定のＩＤが設定されている。「形式１２」には、第１世代の複製を行う利用形式を示す情報（”第１世代複製”）が設定されている。第１世代複製

は、図１４Ａに示したように、オリジナルのコンテンツから、複数の第１世代の複製を作成することができる。ただし、第１世代の複製から第２世代の複製を作成することはできない（許可されていない）。「パラメータ１２」には、”第１世代複製”に対応する所定の情報が設定されている。「管理移動許可情報１２」には、コンテンツの管理移動が許可されていないことを示す情報（”不可”）が設定されている。

「利用内容１３」において、その「ＩＤ１３」には、「利用内容１３」に割り当てられた所定のＩＤが設定されている。「形式１３」には、所定の期間（時間）に限って再生する利用形式を示す情報（”期間制限再生”）が設定され、「パラメータ１３」には、”期間制限再生”に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報１３」には、”不可”が設定されている。

「利用内容１４」において、その「ＩＤ１４」には、「利用内容１４」に割り当てられた所定のＩＤが設定されている。「形式１４」には、５回の複製を行う利用形式（いわゆる、５回複製することができる回数券）を示す情報（”Ｐａｙ Ｐｅｒ　Ｃｏｐｙ５”）が設定されている。なお、この場合も、図１４のＢに示すように、複製からの複製を作成することはできない（許可されていない）。「パラメータ１４」には、複製が５回可能であることを示す情報（”複製５回”）が設定されている。「管理移動許可情報１４」には、”不可”が設定されている。

図１２ＢのＵＣＰＢには、２つの「利用内容２１」、および「利用内容２２」が設けられている。「利用内容２１」において、その「ＩＤ２１」には、「利用内容２１」に割り当てられた所定のＩＤが設定されている。「形式２１」には、４回の再生を行う利用形式を示す情報（”Ｐａｙ　Ｐｅｒ　Ｐｌａｙ４”）が設定され、「パラメータ２１」には、再生が４回可能であることを示す情報（”再生４回”）が設定されている。「管理移動許可情報２１」には、”不可”が設定されている。

「利用内容２２」において、その「ＩＤ２２」には、「利用内容２２」に割り

当てられた所定のＩＤが設定されている。「形式２２」には、”Ｐａｙ　Ｐｅｒ　Ｃｏｐｙ２”が設定され、「パラメータ２２」には、”複製２回”が設定されている。「管理移動許可情報２２」には、”不可”が設定されている。

ここで、ＵＣＰＡおよびＵＣＰＢの内容を比較すると、２００ポイント以上の利用ポイントを有するユーザは、４通りの利用内容１１乃至利用内容１４から利用内容を選択することができるのに対して、２００ポイントより少ない利用ポイントを有するユーザは、２通りの利用内容２１，２２からしか利用内容を選択することができないものとされている。

ところで、図１２は、ＵＣＰＡおよびＵＣＰＢを模擬的に表しているが、例えば、ＵＣＰＡの「利用条件１０」およびＵＣＰＢの「利用条件２０」には、実際は、図１５Ａに示すサービスコード、および図１５Ｂに示すコンディションコードの他、サービスコードに対応して数値や所定の種類を示すバリューコードがそれぞれ設定されている。

図１６Ａは、ＵＣＰＡ（図１２Ａ）の「利用条件１０」の「ユーザ条件１０」および「機器条件１０」として設定されている各コードのコード値を表している。ＵＣＰＡの「利用条件１０」の「ユーザ条件１０」は、”２００ポイント以上”とされているので、”利用ポイントに関し条件有り”を意味する８０ｘｘｈのサービスコード（図１５Ａ）が、このとき数値２００を示す０００Ｃ８ｈのバリューコードが、そして”＞＝（以上）”を意味する０６ｈのコンディションコード（図１５Ｂ）が、ユーザ条件として設定されている。

ＵＣＰＡの「機器条件１０」は、”条件なし”とされているので、”条件なし”を意味する００００ｈのサービスコード（図１５Ａ）が、このとき何ら意味を持たないＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコード（図１５Ｂ）が、機器条件として設定されている。

図１６Ｂは、ＵＣＰＢの「利用条件２０」の「ユーザ条件２０」および「機器条件２０」として設定されている各コードのコード値を表している。「ユーザ条件２０」は、”２００ポイントより少ない”とされているので、”利用ポイント

に関し条件有り”を意味する８０ｘｘｈのサービスコード（図１５Ａ）が、数値２００を示す００００Ｃ８ｈのバリューコードが、そして”＜（より小さい）”を意味する０３ｈのコンディションコード（図１５Ｂ）が、ユーザ条件として設定されている。

ＵＣＰＢの「機器条件２０」は、ＵＣＰＡの「機器条件１０」と同様に、”条件なし”とされ、同一のコード値が設定されているので、その説明は省略する。

図１１に戻り、セキュアコンテナ作成部３８は、例えば、図１７に示すような、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、ＵＣＰＡ，Ｂ、および署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ（この場合、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびＵＣＰＡ，Ｂの全体）にハッシュ関数を適用して得られたハッシュ値が、コンテンツプロバイダの公開鍵暗号の秘密鍵（この場合、コンテンツプロバイダ２－１の秘密鍵Ｋｓｃｐ）で暗号化されたものである。

セキュアコンテナ作成部３８はまた、コンテンツプロバイダセキュアコンテナに、図１８に示すコンテンツプロバイダ２－１の証明書を付してサービスプロバイダ３に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ２－１に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ２－１の名前、コンテンツプロバイダ２－１の公開鍵Ｋｐｃｐ、並びにその署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）から構成されている。

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値とし

て出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、ＭＤ４（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ），ＭＤ５，ＳＨＡ（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ）－１などが用いられる。

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

公開鍵暗号の中で代表的なＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）暗号を、簡単に説明する。まず、２つの十分に大きな素数であるｐおよびｑを求め、さらにｐとｑの積であるｎを求める。（ｐ－１）と（ｑ－１）の最小公倍数Ｌを算出し、更に、３以上Ｌ未満で、かつ、Ｌと互いに素な数ｅを求める（すなわち、ｅとＬを共通に割り切れる数は、１のみである）。

次に、Ｌを法とする乗算に関するｅの乗法逆元ｄを求める。すなわち、ｄ、ｅ、およびＬの間には、ｅｄ＝１　ｍｏｄ　Ｌが成立し、ｄはユークリッドの互除法で算出できる。このとき、ｎとｅが公開鍵とされ、ｐ，ｑ,およびｄが、秘密鍵とされる。

暗号文Ｃは、平文Ｍから、式（１）の処理で算出される。

$C = M^{e} \mod n$ （1）

暗号文Ｃは、式（２）の処理で平文Ｍに、復号される。

$M = C^{d} \mod n$ （2）

証明は省略するが、ＲＳＡ暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式（３）が成立するからである。

$M = C^{d} = (M^{e})^{d} = M^{ed} = M \mod n$ （3）

秘密鍵ｐとｑを知っているならば、公開鍵ｅから秘密鍵ｄは算出できるが、公開鍵ｎの素因数分解が計算量的に困難な程度に公開鍵ｎの桁数を大きくすれば、公開鍵ｎを知るだけでは、公開鍵ｅから秘密鍵ｄは計算できず、復号できない。以上のように、ＲＳＡ暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

また、公開鍵暗号の他の例である楕円曲線暗号（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｃｒｙｐｔｏｇｒａｐｈｙ）についても、簡単に説明する。

楕円曲線$y^{2} = x^{3} + ax + b$上の、ある点をＢとする。楕円曲線上の点の加算を定義し、ｎＢは、Ｂをｎ回加算した結果を表す。同様に、減算も定義する。ＢとｎＢからｎを算出することは、困難であることが証明されている。ＢとｎＢを公開鍵とし、ｎを秘密鍵とする。乱数ｒを用いて、暗号文Ｃ１およびＣ２は、平文Ｍから、公開鍵で式（４）および式（５）の処理で算出される。

$C1 = M + rnB$ （4）

$C2 = rB$ （5）

暗号文Ｃ１およびＣ２は、式（６）の処理で平文Ｍに、復号される。

$$M = C1 - nC2 \qquad (6)$$

復号できるのは、秘密鍵ｎを有するものだけである。以上のように、ＲＳＡ暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

図１１に、再び戻り、コンテンツプロバイダ２－１の相互認証部３９は、ＥＭＤサービスセンタ１から配送用鍵Ｋｄの供給を受けるのに先立ち、ＥＭＤサービスセンタ１と相互認証する。また相互認証部３９は、サービスプロバイダ３へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ３と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコンテナには、秘密しなければならない情報が含まれていないので、この相互認証は必ずしも必要とされるわけではない。

コンテンツプロバイダ２－２は、コンテンツプロバイダ２－１と基本的の同様の構成を有しているので、その図示および説明は省略する。

（４）サービスプロバイダ

次に、図１９のブロック図を参照して、サービスプロバイダ３－１の機能的構成を説明する。コンテンツサーバ４１は、コンテンツプロバイダ２から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ（コンテンツ鍵Ｋｃｏで暗号化されている）、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）、ＵＣＰ、およびコンテンツプロバイダ２の署名を記憶し、セキュアコンテナ作成部４４に供給する。

値付け部４２は、コンテンツプロバイダ２から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証するが、この場合、コンテンツプロバイダ２の証明書が

検証され、正当であるとき、コンテンツプロバイダ２の公開鍵が取得される。そしてこの取得された公開鍵に基づいて、コンテンツプロバイダセキュアコンテナの正当性が検証される。

コンテンツプロバイダセキュアコンテナの正当性を確認すると、値付け部４２は、コンテンツプロバイダセキュアコンテナに含まれるＵＣＰに対応する、ＰＴを作成し、セキュアコンテナ作成部４４に供給する。図２０は、図１２（Ａ）のＵＣＰＡに対応して作成された、２つのＰＴＡ－１（図２０Ａ）およびＰＴＡ－２（図２０Ｂ）を表している。ＰＴには、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「サービスプロバイダのＩＤ」、「ＰＴのＩＤ」、「ＰＴの有効期限」、「価格条件」、および「価格内容」の各項目に対応する所定の情報が含まれる。

ＰＴの、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、および「ＵＣＰのID」には、ＵＣＰに対応する項目の情報が、それぞれ設定される。すなわち、ＰＴＡ－１およびＰＴＡ－２のそれぞれの「コンテンツのＩＤ」には、コンテンツＡのＩＤが、それぞれの「コンテンツプロバイダのＩＤ」には、コンテンツプロバイダ２－１のＩＤが、そしてそれぞれの「ＵＣＰのＩＤ」には、ＵＣＰＡのＩＤが設定されている。

「サービスプロバイダのＩＤ」には、ＰＴの提供元のサービスプロバイダ２のＩＤが設定される。ＰＴＡ－１およびＰＴＡ－２のそれぞれの「サービスプロバイダのＩＤ」には、サービスプロバイダ３－１のＩＤが設定されている。「ＰＴのＩＤ」には、各ＰＴに割り当てられた所定のＩＤが設定される。ＰＴＡ－１の「ＰＴのＩＤ」には、ＰＴＡ－１のＩＤが、ＰＴＡ－２の「ＰＴのＩＤ」には、ＰＴＡ－２のＩＤがそれぞれ設定されている。「ＰＴの有効期限」には、ＰＴの有効期限を示す情報が設定される。ＰＴＡ－１の「ＰＴの有効期限」には、ＰＴＡ－１の有効期限が、ＰＴＡ－２の「ＰＴの有効期限」には、ＰＴＡ－２の有効期限が設定されている。

「価格条件」には、ＵＣＰの「利用条件」と同様に、「ユーザ条件」および「機

器条件」の各項目に対応する所定の情報が設定されている。「価格条件」の「ユーザ条件」には、このＰＴを選択することができるユーザの条件を示す情報が設定され、その「機器条件」には、このＰＴを選択することができる機器の条件を示す情報が設定される。

ＰＴＡ－１の場合、「価格条件１０」が設定され、「価格条件１０」の「ユーザ条件１０」には、ユーザが男性であるを示す情報（”男性”）が設定され、その「機器条件１０」には、”条件なし”が設定されている。すなわち、ＰＴＡ－１は、男性のユーザのみが選択可能となる。

ＰＴＡ－１の「価格条件１０」の「ユーザ条件１０」および「機器条件１０」も、実際は、図２１Ａに示すように、各種コードのコード値が設定されている。「価格条件１０」の「ユーザ条件１０」には、”性別条件有り”を意味する０１ｘｘｈのサービスコード（図１５Ａ）が、このとき男性を意味する０００００ｈのバリューコードが、そして”＝”を意味する０１ｈのコンディションコード（図１５Ｂ）が設定されている。「機器条件１０」には、”条件なし”を意味する００００ｈのサービスコードが、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコードが設定されている。

ＰＴＡ－２の場合、「価格条件２０」が設定され、「価格条件２０」の「ユーザ条件２０」には、ユーザが女性であることを示す情報（”女性”）が設定され、その「機器条件２０」には、”条件なし”が設定されている。すなわち、ＰＴＡ－２は、女性のユーザのみが選択可能となる。

ＰＴＡ－２の「価格条件２０」の「ユーザ条件２０」および「機器条件２０」も、実際は、図２１Ｂに示すように、各コードのコード値が設定されている。「価格条件２０」の「ユーザ条件２０」には、”性別条件有り”を意味する０１ｘｘｈのサービスコード（図１５Ａ）が、この場合女性を示す０００００１ｈのバリューコードが、そして”＝”を意味する０１ｈのコンディションコード（図１５Ｂ）が設定されている。その「機器条件２０」には、”条件なし”を意味する

０００００ｈのサービスコードが、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコードが設定されている。

図２０に戻り、ＰＴの「価格内容」には、コンテンツが、対応するＵＣＰの「利用内容」の「形式」に設定されている利用形式で利用される場合の利用料金が示されている。すなわち、ＰＴＡ－１の「価格内容１１」に設定された”２０００円”およびＰＴＡ－２の「価格内容２１」に設定された”１０００円”は、ＵＣＰＡ（図１２Ａ）の「利用内容１１」の「形式１１」が”買い取り再生”とされているので、コンテンツＡの買い取り価格（料金）を示している。

ＰＴＡ－１の「価格内容１２」の”６００円”およびＰＴＡ－２の「価格内容２２」の”３００円”は、ＵＣＰＡの「利用内容１２」の「形式１２」より、第１世代複製の利用形式でコンテンツＡを利用する場合の料金を示している。ＰＴＡ－１の「価格内容１３」の”１００円”およびＰＴＡ－２の「価格内容２３」の”５０円”は、ＵＣＰＡの「利用内容１３」の「形式１３」より、期間制限再生の利用形式でコンテンツＡを利用する場合の料金を示している。ＰＴＡ－１の「価格内容１４」の”３００円”およびＰＴＡ－２の「価格内容２４」の”１５０円”は、ＵＣＰＡの「利用内容１４」の「形式１４」より、５回の複製を行う利用形式でコンテンツＡを利用する場合の料金を示している。

なお、この例の場合、ＰＴＡ－１（男性ユーザに適用される）の価格内容と、ＰＴＡ－２（女性ユーザに適用される）の価格内容を比較すると、ＰＴＡ－１の価格内容に示される価格が、ＰＴＡ－２の価格内容に示される価格の２倍に設定されている。例えば、ＵＣＰＡの「利用内容１１」に対応するＰＴＡ－１の「価格内容１１」が”２０００円”とされているのに対し、同様にＵＣＰＡの「利用内容１１」に対応するＰＴＡ－２の「価格内容２１」は”１０００円”とされている。同様に、ＰＴＡ－１の「価格内容１２」乃至「価格内容１４」に設定されている価格は、ＰＴＡ－２の「価格内容２２」乃至「価格内容２４」に設定されている価格の２倍とされている。すなわち、コンテンツＡは、女性のユーザがよ

り低価格で利用できるコンテンツとされている。

図２２は、図１２ＢのＵＣＰＢに対応して作成された、２つのＰＴＢ－１およびＰＴＢ－２を表している。図２２ＡのＰＴＢ－１には、コンテンツＡのＩＤ、コンテンツプロバイダ２－１のＩＤ、ＵＣＰＢのＩＤ、サービスプロバイダ３－１のＩＤ、ＰＴＢ－１のＩＤ、ＰＴＢ－１の有効期限、価格条件３０、２通りの価格内容３１，３２などが含まれている。

ＰＴＢ－１の「価格条件３０」の「ユーザ条件３０」には”条件なし”が設定され、「機器条件３０」には、機器が従機器であることを条件とする情報（”従機器”）が設定されている。すなわち、ＰＴＢ－１は、コンテンツＡが従機器において利用される場合にのみ選択可能となる。

ＰＴＢ－１の「価格条件３０」の「ユーザ条件３０」および「機器条件３０」にも、実際は、図２３Ａに示すように、各コードのコード値が設定されている。「ユーザ条件３０」には、”条件なし”を意味する０００００ｈのサービスコード（図１５Ａ）が、この場合何ら意味を持たないＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコード（図１５Ｂ）が設定されている。「機器条件３０」は、”従機器”とされているので、”機器に関し条件有り”を意味する００ｘｘｈのサービスコードが、このとき”数値１００”を示す０００００６４ｈのバリューコードが、そして”＜（小さい）”を意味する０３ｈのコンディションコードが設定されている。この例の場合、従機器には、１００番より小さい機器番号が設定されているので、このようなコード値が設定される。

ＰＴＢ－１の「価格内容３１」の”１００円”は、ＵＣＰＢ（図１２Ｂ）の「利用内容２１」の「形式２１」が”Ｐａｙ　Ｐｅｒ　Ｐｌａｙ４”とされているので、４回の再生を行う場合の料金を示し、「価格内容３２」の”３００円”は、ＵＣＰＢの「利用内容２２」の「形式２２」が”Ｐａｙ　Ｐｅｒ　Ｃｏｐｙ２”とされているので、２回の複製を行う場合の料金を示している。

ＵＣＰＢに対応して作成された、もう一方のＰＴＢ－２には、図２２Ｂに示す

ように、コンテンツＡのＩＤ、コンテンツプロバイダ２－１のＩＤ、ＵＣＰＢのＩＤ、サービスプロバイダ３－１のＩＤ、ＰＴＢ－２のＩＤ、ＰＴＢ－２の有効期限、価格条件４０、および２通りの価格内容４１，４２などが含まれている。

ＰＴＢ－２の「価格条件４０」の「ユーザ条件４０」には”条件なし”が設定され、その「機器条件４０」には、機器が主機器であることを条件とする情報（”主機器”）が設定されている。すなわち、ＰＴＢ－２は、主機器においてコンテンツが利用される場合にのみ選択可能となる。

ＰＴＢ－２の「価格条件４０」の「ユーザ条件４０」および「機器条件４０」にも、実際は、図２３Ｂに示すように、各コードのコード値が設定されている。「価格条件４０」の「ユーザ条件４０」には、”条件なし”を意味する０００００ｈのサービスコード（図１５Ａ）が、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコード（１５Ｂ）が設定されている。「機器条件４０」には、”機器に関し条件有り”を意味する００ｘｘｈのサービスコードが、このとき”数値１００”を示す０００６４ｈのバリューコードが、そして”＝＞（以上）”を意味する０６ｈのコンディションコードが設定されている。この例の場合、主機器には、１００番以上の機器番号が設定されているので、このようなコード値が設定される。

ＰＴＢ－２の「価格内容４１」および「価格内容４２」のそれぞれに示される価格は、ＵＣＰＢの「利用内容２１」の「形式２１」および「利用内容２２」の「形式２２」のそれぞれに示される利用形式でコンテンツＡを利用する場合の料金を示している。

ここで、ＰＴＢ－１（従機器に適用される）の価格内容とＰＴＢ－２（主機器に適用される）の価格内容を比較すると、ＰＴＢ－１の価格内容は、ＰＴＢ－２の価格内容の２倍に設定されている。例えば、ＰＴＢ－１の「価格内容３１」が”１００円”とされているのに対し、ＰＴＢ－２の「価格内容４１」は５０円とされており、「価格内容３２」が”３００円”とされているのに対して、「価格内容４２」は”１５０円”とされている。

図１９に戻り、ポリシー記憶部４３は、コンテンツプロバイダ２から供給された、コンテンツのＵＣＰを記憶し、セキュアコンテナ作成部４４に供給する。

セキュアコンテナ作成部４４は、例えば、図２４に示すような、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、ＵＣＰＡ，Ｂ、コンテンツプロバイダ２の署名、ＰＴＡ－１，Ａ－２，Ｂ－１，Ｂ－２、およびサービスプロバイダ３の署名からなるサービスプロバイダセキュアコンテナを作成する。

セキュアコンテナ作成部４４はまた、作成したサービスプロバイダセキュアコンテナを、図２５に示すような、証明書のバージョン番号、認証局がサービスプロバイダ３－１に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３－１の名前、サービスプロバイダ３－１の公開鍵Ｋｐｓｐ、並びに認証局の署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク５に供給する。

図１９に、再び戻り、相互認証部４５は、コンテンツプロバイダ２からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ２と相互認証する。相互認証部４５また、ユーザホームネットワーク５へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク５と相互認証するが、このサービスプロバイダ３とユーザホームネットワーク５との相互認証は、例えば、ネットワーク４が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ３は、コンテンツプロバイダ２およびユーザホームネットワーク５と相互認証を行わなくてもよい。

サービスプロバイダ３－２の構成は、サービスプロバイダ３－１の構成と基本的に同様であるので、その図示および説明は省略する。

（５）ユーザホームネットワーク

（５－１）レシーバ５１

次に、図２６のブロック図を参照して、ユーザホームネットワーク５を構成するレシーバ５１の構成例を説明する。レシーバ５１は、通信部６１、ＳＡＭ６２、外部記憶部６３、伸張部６４、通信部６５、インタフェース６６、表示制御部６７、および入力制御部６８より構成されている。通信部６１は、ネットワーク４を介してサービスプロバイダ３、またはＥＭＤサービスセンタ１と通信し、所定の情報を受信し、または送信する。

ＳＡＭ６２は、相互認証モジュール７１、課金処理モジュール７２、記憶モジュール７３、復号／暗号化モジュール７４、およびデータ検査モジュール７５からなるが、シングルチップの暗号処理専用ＩＣで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有している。

ＳＡＭ６２の相互認証モジュール７１は、記憶モジュール７３に記憶されている、図２７に示すＳＡＭ６２の証明書を、相互認証相手に送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵Ｋｔｅｍｐ（セッション鍵）を復号／暗号化モジュール７４に供給する。ＳＡＭの証明書には、コンテンツプロバイダ２－１の証明書およびサービスプロバイダ３－１の証明書に含まれている情報に対応する情報が含まれているので、その説明は省略する。

課金処理モジュール７２は、選択されたＵＣＰの利用内容に基づいて、使用許諾条件情報ＵＣＳおよびコンテンツが“買い取り再生”の利用形式で権利購入された場合のＵＣＳの例であり、課金情報を作成する。図２８は、図１２Ａに示したＵＣＰＡの利用内容１１と、図２０Ａに示したＰＴＡ－１の価格内容１１に基づいて作成されたＵＣＳＡを表している。ＵＣＳには、図２８に示されるように、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「ＵＣＰの有効期限」、「サービスプロバイダのＩＤ」、「ＰＴのＩＤ」、「ＰＴの有効期限」、「ＵＣＳのＩＤ」、「ＳＡＭのＩＤ」、「ユーザのＩＤ」、

「利用内容」、および「利用履歴」の各項目に対応する所定の情報が設定される。

ＵＣＳの、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「ＵＣＰの有効期限」、「サービスプロバイダのＩＤ」、「ＰＴのＩＤ」、および「ＰＴの有効期限」の各項目には、ＰＴの、それらに対応する項目の情報が設定される。すなわち、図２８のＵＣＳＡの、「コンテンツのＩＤ」には、コンテンツＡのＩＤが、「コンテンツプロバイダのＩＤ」には、コンテンツプロバイダ２－１のＩＤが、「ＵＣＰのＩＤ」には、ＵＣＰＡのＩＤが、「ＵＣＰの有効期限」には、ＵＣＰＡの有効期限が、「サービスプロバイダのＩＤ」には、サービスプロバイダ３－１のＩＤが、「ＰＴのＩＤ」には、ＰＴＡ－１のＩＤが、そして「ＰＴの有効期限」には、ＰＴＡ－１の有効期限が、それぞれ設定されている。

「ＵＣＳのＩＤ」には、ＵＣＳに割り当てられた所定のＩＤが設定され、ＵＣＳＡの「ＵＣＳのＩＤ」には、ＵＣＳＡのＩＤが設定されている。「ＳＡＭのＩＤ」には、機器のＳＡＭのＩＤが設定され、ＵＣＳＡの「ＳＡＭのＩＤ」には、レシーバ５１のＳＡＭ６２のＩＤが設定されている。「ユーザのＩＤ」には、コンテンツを利用するユーザのＩＤが設定され、ＵＣＳＡの「ユーザのＩＤ」には、ユーザＦのＩＤが設定されている。

「利用内容」は、「ＩＤ」、「形式」、「パラメータ」、および「管理移動状態情報」の各項目からなり、そのうち「ＩＤ」、「形式」、および「パラメータ」の項目には、選択されたＵＣＰの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、ＵＣＳＡの「ＩＤ」には、ＵＣＰＡの「利用内容１１」の「ＩＤ１１」に設定されている情報（利用内容１１のＩＤ）が、「形式」には、「利用内容１１」の「形式１１」に設定されている”買い取り再生”が、「パラメータ」には、「利用内容１１」の「パラメータ１１」に設定されている情報（”買い取り再生”に対応する情報）が設定されている。

「利用内容」の「管理移動状態情報」には、選択されたＵＣＰの「管理移動許

可情報」に”可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれのＩＤが設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器のＩＤが、管理移動先の機器のＩＤとしても設定される。一方、ＵＣＰの「管理移動許可情報」に、”不可”が設定されている場合、「管理移動状態情報」には”不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われない（許可されない）。ＵＣＳＡの「管理移動状態情報」には、ＵＣＰＡの「利用内容１１」の「管理移動許可情報１１」に”可”が設定されており、また、このとき、コンテンツＡは管理移動されていないので、ＳＡＭ６２のＩＤが、管理移動元の機器のＩＤおよび管理移動先の機器のＩＤとして設定されている。

「利用履歴」には、同一のコンテンツに対する利用形式の履歴が設定される。ＵＣＳＡの「利用履歴」には、”買い取り再生”を示す情報のみが記憶されているが、例えば、レシーバ５１において、コンテンツＡが以前に利用されていた場合、そのときの利用形式も記憶される。

なお、上述したＵＣＳにおいては、「ＵＣＰの有効期限」および「ＰＴの有効期限」が設けられているがそれらをＵＣＳに設定しないようにすることもできる。また、上述したＵＣＳにおいて、「コンテンツプロバイダのＩＤ」が設けられているが、ＵＣＰのＩＤがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのＩＤ」も同様に、ＰＴのＩＤがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

作成されたＵＣＳは、レシーバ５１の復号／暗号化モジュール７４の復号化ユニット９１から供給されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）とともに、外部記憶部６３に送信され、その利用情報記憶部６３Ａに記憶される。外部記憶部６３の利用情報記憶部６３Ａは、図２９に示すように、

M個のブロックＢＰ－１乃至ＢＰ－Mに分割され（例えば、１メガバイト毎に分割され）、各ブロックＢＰが、Ｎ個の利用情報用メモリ領域ＲＰ－１乃至ＲＰ－Ｎに分割されている。ＳＡＭ６２から供給されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）およびＵＣＳは、利用情報用記憶部６３Ａの所定のブロックＢＰの利用情報用メモリ領域ＲＰに、対応して記憶される。

図２９の例では、ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－３に、図２８に示したＵＣＳＡと、コンテンツＡを復号するためのコンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）が対応して記憶されている。ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－１，ＲＰ－２には、他のコンテンツ鍵Ｋｃｏ１，Ｋｃｏ２（それぞれ保存用鍵Ｋｓａｖｅで暗号化されている）およびＵＣＳ１，２がそれぞれ記憶されている。ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－４（図示せず）乃至ＲＰ－Ｎ、およびブロックＢＰ－２（図示せず）乃至ＢＰ－Mには、この場合、コンテンツ鍵ＫｃｏおよびＵＣＳは記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域ＲＰに記憶されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）およびＵＣＳを、個々に区別する必要がない場合、まとめて、利用情報と称する。

図３０は、図２８に示したＵＣＳＡと同時に作成された課金情報Ａを表している。課金情報は、図３０に示されるように、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「ＵＣＰの有効期限」、「サービスプロバイダのＩＤ」、「ＰＴのＩＤ」、「ＰＴの有効期限」、「ＵＣＳのＩＤ」、「ＳＡＭのＩＤ」、「ユーザのＩＤ」、「利用内容」、および「課金履歴」の各項目に対応する所定の情報が設定される。

課金情報の、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「ＵＣＰの有効期限」、「サービスプロバイダのＩＤ」、「ＰＴのＩＤ」、「ＰＴの有効期限」、「ＵＣＳのＩＤ」、「ＳＡＭのＩＤ」、「ユーザのＩＤ」、および「利用内容」には、ＵＣＳの、それらに対応する項目の情報

が、それぞれ設定される。すなわち、図３０の課金情報Ａの、「コンテンツのＩＤ」には、コンテンツＡのＩＤが、「コンテンツプロバイダのＩＤ」には、コンテンツプロバイダ２－１のＩＤが、「ＵＣＰのＩＤ」には、ＵＣＰＡのＩＤが、「ＵＣＰの有効期限」には、ＵＣＰＡの有効期限が、「サービスプロバイダのＩＤ」には、サービスプロバイダ３－１のＩＤが、「ＰＴのＩＤ」には、ＰＴＡ－１のＩＤが、「ＰＴの有効期限」には、ＰＴＡ－１の有効期限が、「ＵＣＳのＩＤ」には、ＵＣＳＡのＩＤが、「ＳＡＭのＩＤ」には、ＳＡＭ６２のＩＤが、「ユーザのＩＤ」には、ユーザＦのＩＤが、そして「利用内容」には、ＵＣＳＡの「利用内容１１」の内容が、それぞれ設定されている。

課金情報の「課金履歴」には、機器において計上された課金の合計額を示す情報が設定される。課金情報Ａの「課金履歴」には、レシーバ５１において計上された課金の合計額が設定されている。

なお、上述した課金情報においては、「ＵＣＰの有効期限」および「ＰＴの有効期限」が設けられているが、それらを課金情報に設定しないようにすることもできる。また、上述した課金情報においては、「コンテンツプロバイダのＩＤ」が設けられているが、ＵＣＰのＩＤがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのＩＤ」も同様に、ＰＴのＩＤがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

図２６に戻り、記憶モジュール７３には、図３１に示すように、ＳＡＭ６２の公開鍵Ｋｐｕ、ＳＡＭ６２の秘密鍵Ｋｓｕ、ＥＭＤサービスセンタ１の公開鍵Ｋｐｅｓｃ、認証局の公開鍵Ｋｐｃａ、保存用鍵Ｋｓａｖｅ、３ヶ月分の配送用鍵Ｋｄなどの各種鍵、ＳＡＭ６２の証明書（図２７）、課金情報（例えば、図３０の課金情報Ａ）、基準情報５１、およびM個の検査値ＨＰ－１乃至ＨＰ－Ｍなどが記憶されている。

図３２は、記憶モジュール７３に記憶されている基準情報５１を表している。

基準情報には、「ＳＡＭのＩＤ」、「機器番号」、「決済ＩＤ」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項目に設定される所定情報などが含まれている。

基準情報の、「ＳＡＭのＩＤ」、「機器番号」、「決済ＩＤ」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」には、ＥＭＤサービスセンタ１のユーザ管理部１８により管理されるシステム登録情報（図９）の、それらに対応する項目の情報が、それぞれ設定される。すなわち、基準情報５１には、ＳＡＭ６２のＩＤ、ＳＡＭ６２の機器番号（１００番）、ユーザＦの決済ＩＤ、ユーザＦの決済ユーザ情報（ユーザＦの一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザＦのＩＤ、およびユーザＦのパスワード）、および図３３に示す利用ポイント情報（図１０に示したものと同様の情報）が設定されている。

「課金の上限額」には、機器がＥＭＤシステムに正式登録されている状態と仮登録されている状態で、それぞれ異なる課金の上限額が設定される。基準情報５１の「課金の上限額」には、レシーバ５１が正式登録されているので、正式登録されている状態における課金の上限額を示す情報（”正式登録時の上限額”）が設定されている。なお、正式登録されている状態における課金の上限額は、仮登録されている状態における課金の上限額よりも、大きな額である。

次に、記憶モジュール７３に記憶される、図３１に示したＭ個の検査値ＨＰ－１乃至ＨＰ－Ｍについて説明する。検査値ＨＰ－１は、外部記憶部６３の利用情報記憶部６３Ａのブロック ＢＰ－１に記憶されているデータの全体にハッシュ関数が適用されて算出されたハッシュ値である。検査値ＨＰ－２乃至ＨＰ－Ｍも、検査値ＨＰ－１と同様に、外部記憶部６３の、対応するブロックＢＰ－２乃至ＢＰ－Ｍのそれぞれに記憶されているデータのハッシュ値である。

図２６に戻り、ＳＡＭ６２の復号／暗号化モジュール７４は、復号ユニット９１、乱数発生ユニット９２、および暗号化ユニット９３から構成される。復号ユニット９１は、暗号化されたコンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、暗号

化ユニット９３に出力する。乱数発生ユニット９２は、必要に応じ（例えば、相互認証時に）、所定の桁数の乱数を発生し、一時鍵Ｋｔｅｍｐを生成し、暗号化ユニット９３に出力する。

暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを、再度、記憶モジュール７３に保持されている保存用鍵Ｋｓａｖｅで暗号化する。暗号化されたコンテンツ鍵Ｋｃｏは、外部記憶部６３に供給される。暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを伸張部６４に送信するとき、コンテンツ鍵Ｋｃｏを乱数発生ユニット９２で生成した一時鍵Ｋｔｅｍｐで暗号化する。

データ検査モジュール７５は、記憶モジュール７３に記憶されている検査値ＨＰと、外部記憶部６３の利用情報記憶部６３Ａの、対応するブロックＢＰのデータのハッシュ値を比較し、ブロックＢＰのデータが改竄されていないか否かを検査する。データ検査モジュール７５はまた、コンテンツの購入、利用、および管理移動等が行われる際に、検査値ＨＰを算出し、記憶モジュール７３に記憶（更新）させる。

伸張部６４は、相互認証モジュール１０１、復号モジュール１０２、復号モジュール１０３、伸張モジュール１０４、およびウォータマーク付加モジュール１０５から構成される。相互認証モジュール１０１は、ＳＡＭ６２と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール１０２に出力する。復号モジュール１０２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール１０３に出力する。復号モジュール１０３は、ＨＤＤ５２に記録されたコンテンツをコンテンツ鍵Ｋｃｏで復号し、伸張モジュール１０４に出力する。伸張モジュール１０４は、復号されたコンテンツを、更にＡＴＲＡＣ２等の方式で伸張し、ウォータマーク付加モジュール１０５に出力する。ウォータマーク付加モジュール１０５は、コンテンツにレシーバ５１を特定するための情報（例えば、ＳＡＭ６２のＩＤ）のウォータマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

通信部６５は、ユーザホームネットワーク５のレシーバ２０１との通信処理を

行う。インターフェース６６は、ＳＡＭ６２および伸張部６４からの信号を所定の形式に変更し、ＨＤＤ５２に出力し、また、ＨＤＤ５２からの信号を所定の形式に変更し、ＳＡＭ６２および伸張部６４に出力する。

表示制御部６７は、表示部（図示せず）への出力を制御する。入力制御部６８は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

ＨＤＤ５２は、サービスプロバイダ３から供給されたコンテンツの他、図３４に示すような登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象ＳＡＭ情報部より構成されている。

対象ＳＡＭ情報部には、この登録リストを保有する機器のＳＡＭＩＤ、この例の場合、レシーバ５１のＳＡＭ６２のＩＤが（「対象ＳＡＭＩＤ」の欄に）記憶されている。対象ＳＡＭ情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ５１は、レシーバ２０１に接続されているので、自分自身を含む値２が（「接続されている機器数」の欄に）記憶されている。

リスト部は、「ＳＡＭ　ＩＤ」、「ユーザＩＤ」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態フラグ」、「登録条件署名」、および「登録リスト署名」の９個の項目から構成され、この例の場合、レシーバ５１の登録条件として、それぞれの項目に所定の情報が記憶されている。

「ＳＡＭ　ＩＤ」には、機器のＳＡＭのＩＤが記憶される。この例の場合、レシーバ５１のＳＡＭ６２のＩＤおよびレシーバ２０１のＳＡＭ２１２のＩＤが記憶されている。「ユーザＩＤ」には、対応する機器のユーザのＩＤが記憶される。この例の場合、ユーザＦのＩＤおよびユーザＡのＩＤが記憶されている。

「購入処理」には、対応する機器が、コンテンツを購入（正確には、コンテンツを利用する権利を購入）するための処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ５１およびレ

シーバ２０１は、コンテンツを購入するための処理を行うことができるので、”可”が記憶されている。

「課金処理」には、対応する機器が、ＥＭＤサービスセンタ１との間で、課金を決済する処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ５１は、ユーザＦが決済ユーザとして登録されており、レシーバ２０１は、ユーザＡが決済ユーザとして登録されているので、課金を決済する処理を行うことができる。そのため、「課金処理」には、”可”が記憶されている。

「課金機器」には、対応する機器において計上された課金に対する課金を決済する処理を行う機器のＳＡＭのＩＤが記憶される。この例の場合、レシーバ５１（ＳＡＭ６２）およびレシーバ２０１（ＳＡＭ２１２）は、自分自身の課金に対する決済を行うことができるので、ＳＡＭ６２のＩＤおよびＳＡＭ２１２のＩＤが記憶されている。

「コンテンツ供給機器」には、対応する機器が、コンテンツの供給をサービスプロバイダ３からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のＳＡＭのＩＤが記憶される。この例の場合、レシーバ５１およびレシーバ２０１は、コンテンツの供給をサービスプロバイダ３から受けるので、コンテンツを供給する機器が存在しない旨を示す情報（”なし”）が記憶されている。なお、ここで意味するコンテンツの供給は、管理移動によるものは含まれない。

「状態フラグ」には、対応する機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（”制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（”制限あり”）、また動作が停止させられている場合には、その旨を示す情報（”停止”）が記憶される。例えば、決済が成功しなかった場合、その機器に対応する「状態フラグ」には、”制限あり”が設定される。この例の場合、「状態フラグ」に”制限あり”が設定された機器においては、すでに購入されたコンテンツを利用する処理は実行されるが、新たなコ

ンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、”停止”が設定され、機器の動作が停止される。これにより、その機器はＥＭＤシステムからのサービスを、一切受けることができなくなる。

この例の場合、レシーバ５１およびレシーバ２０１に対しては、何ら制限が課せられていないものとし、「状態フラグ」には”なし”が設定されている。

「登録条件署名」には、登録条件として、それぞれ、「ＳＡＭＩＤ」、「ユーザＩＤ」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するＥＭＤサービスセンタ１による署名が記憶されている。この例の場合、レシーバ５１およびレシーバ２０１の登録条件に対する署名が記憶されている。

「登録リスト署名」には、登録リストに設定されているデータの全体に対する署名が設定されている。

（５－２）レシーバ２０１

図３５は、レシーバ２０１の構成例を表している。レシーバ２０１の通信部２１１乃至入力制御部２１８は、レシーバ５１の通信部６１乃至入力制御部６８と同様の機能を有しているので、その詳細な説明は適宜省略する。

外部記憶部２１３は、図３６に示すように、Ｐ個のブロックＢＭ－１乃至ＢＭ－Ｐに分割され（例えば、１メガバイト毎に分割され）、各ブロックＢＭが、Ｑ個の移動情報用メモリ領域ＲＭ－１乃至ＲＭ－Ｑに分割されている移動情報記憶部２１３Ａを有しており、例えば、コンテンツが管理移動されたとき、ＳＡＭ２１２から送信される、そのコンテンツに対応したコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）、コンテンツのＩＤ、および管理移動元の機器のＳＡＭのＩＤ（以下、個々に区別する必要がない場合、これらをまとめて、移動情報と称する）を記憶する。

図３６の移動情報記憶部２１３ＡのブロックＢＭ－１の移動情報用メモリ領域

ＲＭ－２には、コンテンツＡ（コンテンツ鍵Ｋｃｏで暗号化されている）に対応するコンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）、コンテンツＡのＩＤ、およびＳＡＭ６２のＩＤが記憶されている。すなわち、レシーバ５１から、コンテンツＡが管理移動されている状態の移動情報記憶部２１３Ａを表している。

なお、ブロックＢＭ－１の移動情報用メモリ領域ＲＭ－２（図示せず）乃至ＲＭ－Ｑ、およびブロックＢＭ－２（図示せず）乃至ＢＭ－Ｐには、移動情報が記憶されておらず、空いている（移動情報を記憶することができる）ことを示す初期情報が記憶されている。

ＳＡＭ２１２の記憶モジュール２２３には、図３７に示すように、ＳＡＭ２１２の公開鍵Ｋｐｕ、ＳＡＭ２１２の秘密鍵Ｋｓｕ、ＥＭＤサービスセンタ１の公開鍵Ｋｐｅｓｃ、認証局の公開鍵Ｋｐｃａ、保存用鍵Ｋｓａｖｅ、３ヶ月分の配送用鍵Ｋｄ、予め認証局から配布されているＳＡＭ２１２の証明書、基準情報２０１、およびＱ個の検査値ＨＭ－１乃至ＨＭ－Ｑが記憶されている。

Ｐ個の検索値ＨＭ－１乃至ＨＭ－Ｑは、外部記憶部２１３の移動情報記憶部２１３Ａの、各ブロックＢＭ－１乃至ＢＭ－Ｑの記憶されているデータにハッシュ関数が適用されて算出されたハッシュ値である。

ＨＤＤ２０２は、ＨＤＤ５２と同様の機能を有するので、その説明は省略するが、ＨＤＤ２０２には、図３４のレシーバ５１の登録リストのリスト部に示された、レシーバ５１の登録条件およびレシーバ２０１の登録条件が設定されたリスト部を有するレシーバ２０１の登録リスト（図示せず）が記憶されている。

なお、この例の場合、簡単のために、レシーバ５１の外部記憶部６３には、利用情報記憶部６３Ａのみが設けられ、またレシーバ２０１の外部記憶部２１３には、移動情報記憶部２１３Ａのみが設けられているようにしたが、実際は、レシーバ５１の外部記憶部６３には、利用情報記憶部６３Ａの他、移動情報記憶部（図示せず）も設けられている。同様に、レシーバ２０１の外部記憶部２１３にも、移動情報記憶部２１３Ａの他、利用情報記憶部（図示せず）が設けられている

（６）コンテンツの購入及び利用

次に、ＥＭＤシステムの処理について、図３８のフローチャートを参照して説明するが、ここでは、コンテンツプロバイダ２－１に保持されているコンテンツＡが、サービスプロバイダ３－１を介して、ユーザホームネットワーク５のレシーバ５１に供給され、利用される場合を例として説明する。

（６－１）ＥＭＤサービスセンタからコンテンツプロバイダへの配送用鍵の伝送

ステップＳ１１において、配送用鍵Ｋｄが、ＥＭＤサービスセンタ１からコンテンツプロバイダ２－１に供給される処理が行われる。この処理の詳細は、図３９のフローチャートに示されている。すなわち、ステップＳ３１において、ＥＭＤサービスセンタ１の相互認証部１７（図３）は、コンテンツプロバイダ２－１の相互認証部３９（図１１）と相互認証し、コンテンツプロバイダ２－１が、正当なプロバイダであることが確認した後、ＥＭＤサービスセンタ１のコンテンツプロバイダ管理部１２は、鍵サーバ１４から供給された配送用鍵Ｋｄをコンテンツプロバイダ２－１に送信する。なお、相互認証処理の詳細は、図４０乃至図４２を参照して後述する。

次に、ステップＳ３２において、コンテンツプロバイダ２－１の暗号化部３６は、ＥＭＤサービスセンタ１から送信された配送用鍵Ｋｄを受信し、ステップＳ３３において、配送用鍵Ｋｄを記憶する。

このように、コンテンツプロバイダ２－１の暗号化部３６が、配送用鍵Ｋｄを記憶したとき、処理は終了し、図３８のステップＳ１２に進む。ここで、ステップＳ１２以降の処理の説明の前に、図３９のステップＳ３１における相互認証処理（なりすましがないことを確認する処理）について、１つの共通鍵を用いる場合（図４０）、２つの共通鍵を用いる場合（図４１）、および公開鍵暗号を用いる場合（図４２）を例として説明する。

図４０は、１つの共通鍵で、共通鍵暗号であるＤＥＳを用いる、コンテンツプロバイダ２の相互認証部３９とＥＭＤサービスセンタ１の相互認証部１７との相

互認証の動作を説明するフローチャートである。ステップＳ４１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する（乱数生成部３５が生成するようにしてもよい）。ステップＳ４２において、コンテンツプロバイダ２の相互認証部３９は、ＤＥＳを用いて乱数Ｒ１を、予め記憶している共通鍵Ｋｃで暗号化する（暗号化部３６で暗号化するようにしてもよい）。ステップＳ４３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をＥＭＤサービスセンタ１の相互認証部１７に送信する。

ステップＳ４４において、ＥＭＤサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Kcで復号する。ステップＳ４５において、ＥＭＤサービスセンタ１の相互認証部１７は、３２ビットの乱数Ｒ２を生成する。ステップＳ４６において、ＥＭＤサービスセンタ１の相互認証部１７は、復号した６４ビットの乱数Ｒ１の下位３２ビットを乱数Ｒ２で入れ替え、連接Ｒ1_H‖Ｒ２を生成する。なお、ここでＲｉ$_H$は、Ｒｉの上位ｎビットを表し、Ａ‖Ｂは、ＡとＢの連接（ｎビットのＡの下位に、ｍビットのＢを結合して、（ｎ＋ｍ）ビットとしたもの）を表す。ステップＳ４７において、ＥＭＤサービスセンタ１の相互認証部１７は、ＤＥＳを用いてＲ1_H‖Ｒ２を共通鍵Ｋｃで暗号化する。ステップＳ４８において、ＥＭＤサービスセンタ１の相互認証部１７は、暗号化したＲ1_H‖Ｒ２をコンテンツプロバイダ２に送信する。

ステップＳ４９において、コンテンツプロバイダ２の相互認証部３９は、受信したＲ1_H‖Ｒ２を共通鍵Ｋｃで復号する。ステップＳ５０において、コンテンツプロバイダ２の相互認証部３９は、復号したＲ1_H‖Ｒ２の上位３２ビットＲ1_Hを調べ、ステップＳ４１で生成した、乱数Ｒ１の上位３２ビットＲ1_Hと一致すれば、ＥＭＤサービスセンタ１が正当なセンタであることを認証する。生成した乱数Ｒ1_Hと、受信したＲ1_Hが一致しないとき、処理は終了される。両者が一致するとき、ステップＳ５１において、コンテンツプロバイダ２の相互認証部３９は、３２ビットの乱数Ｒ３を生成する。ステップＳ５２において、コンテンツプロバイダ２の相互認証部３９は、受信し復号したＲ1_H‖Ｒ２から下位３２ビ

ットを取り出した乱数Ｒ２を上位に設定し、生成した乱数Ｒ３をその下位に設定し、連接Ｒ２‖Ｒ３とする。ステップＳ５３において、コンテンツプロバイダ２の相互認証部３９は、ＤＥＳを用いて連接Ｒ２‖Ｒ３を共通鍵Ｋｃで暗号化する。ステップＳ５４において、コンテンツプロバイダ２の相互認証部３９は、暗号化された連接Ｒ２‖Ｒ３をＥＭＤサービスセンタ１の相互認証部１７に送信する。

ステップＳ５５において、ＥＭＤサービスセンタ１の相互認証部１７は、受信した連接Ｒ２‖Ｒ３を共通鍵Kcで復号する。ステップＳ５６において、ＥＭＤサービスセンタ１の相互認証部１７は、復号した連接Ｒ２‖Ｒ３の上位３２ビットを調べ、乱数Ｒ２と一致すれば、コンテンツプロバイダ２を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

図４１は、２つの共通鍵Ｋｃ１，Ｋｃ２で、共通鍵暗号であるＤＥＳを用いる、コンテンツプロバイダ２の相互認証部３９とＥＭＤサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ６１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ６２において、コンテンツプロバイダ２の相互認証部３９は、ＤＥＳを用いて乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で暗号化する。ステップＳ６３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をＥＭＤサービスセンタ１に送信する。

ステップＳ６４において、ＥＭＤサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で復号する。ステップＳ６５において、ＥＭＤサービスセンタ１の相互認証部１７は、乱数Ｒ１を予め記憶している共通鍵Ｋｃ２で暗号化する。ステップＳ６６において、ＥＭＤサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ６７において、ＥＭＤサービスセンタ１の相互認証部１７は、乱数Ｒ２を共通鍵Ｋｃ２で暗号化する。ステップＳ６８において、ＥＭＤサービスセンタ１の相互認証部１７は、暗号化された乱数Ｒ１および乱数Ｒ２をコンテンツプロバイダ２の相互認

証部３９に送信する。

ステップＳ６９において、コンテンツプロバイダ２の相互認証部３９は、受信した乱数Ｒ１および乱数Ｒ２を予め記憶している共通鍵Ｋｃ２で復号する。ステップＳ７０において、コンテンツプロバイダ２の相互認証部３９は、復号した乱数Ｒ１を調べ、ステップＳ６１で生成した乱数Ｒ１（暗号化する前の乱数Ｒ１）と一致すれば、ＥＭＤサービスセンタ１を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップＳ７１において、コンテンツプロバイダ２の相互認証部３９は、復号して得た乱数Ｒ２を共通鍵Ｋｃ１で暗号化する。ステップＳ７２において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ２をＥＭＤサービスセンタ１に送信する。

ステップＳ７３において、ＥＭＤサービスセンタ１の相互認証部１７は、受信した乱数Ｒ２を共通鍵Ｋｃ１で復号する。ステップＳ７４において、ＥＭＤサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ６６で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

図４２は、公開鍵暗号である、１６０ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ２の相互認証部３９とＥＭＤサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ８１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ８２において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐを含む証明書（認証局から予め取得しておいたもの）と、乱数Ｒ１をＥＭＤサービスセンタ１の相互認証部１７に送信する。

ステップＳ８３において、ＥＭＤサービスセンタ１の相互認証部１７は、受信した証明書の署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）を、予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、コンテンツプロバイダ２の公開鍵Ｋｐｃｐとコンテンツプロバイダ２の名前のハッシュ値を取り出すとともに、証

明書に平文のまま格納されているコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵Ｋｐｃｐが改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

適正な認証結果が得られたとき、ステップＳ８４において、ＥＭＤサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ８５において、ＥＭＤサービスセンタ１の相互認証部１７は、乱数Ｒ１および乱数Ｒ２の連接Ｒ１‖Ｒ２を生成する。ステップＳ８６において、ＥＭＤサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を自分自身の秘密鍵Ｋｓｅｓｃで暗号化する。ステップＳ８７において、ＥＭＤサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を、ステップＳ８３で取得したコンテンツプロバイダ２の公開鍵Ｋｐｃｐで暗号化する。ステップＳ８８において、ＥＭＤサービスセンタ１の相互認証部１７は、秘密鍵Ｋｓｅｓｃで暗号化された連接Ｒ１‖Ｒ２、公開鍵Ｋｐｃｐで暗号化された連接Ｒ１‖Ｒ２、および自分自身の公開鍵Ｋｐｅｓｃを含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ２の相互認証部３９に送信する。

ステップＳ８９において、コンテンツプロバイダ２の相互認証部３９は、受信した証明書の署名を予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、正しければ証明書から公開鍵Ｋｐｅｓｃを取り出す。この場合の処理は、ステップＳ８３における場合と同様であるので、その説明は省略する。ステップＳ９０において、コンテンツプロバイダ２の相互認証部３９は、ＥＭＤサービスセンタ１の

秘密鍵Ｋｓｅｓｃで暗号化されている連接Ｒ１‖Ｒ２を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで復号する。ステップＳ９１において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐで暗号化されている連接Ｒ１‖Ｒ２を、自分自身の秘密鍵Ｋｓｃｐで復号する。ステップＳ９２において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で復号された連接Ｒ１‖Ｒ２と、ステップＳ９１で復号された連接Ｒ１‖Ｒ２を比較し、一致すればＥＭＤサービスセンタ１を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

適正な認証結果が得られたとき、ステップＳ９３において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ３を生成する。ステップＳ９４において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で取得した乱数Ｒ２および生成した乱数Ｒ３の連接Ｒ２‖Ｒ３を生成する。ステップＳ９５において、コンテンツプロバイダ２の相互認証部３９は、連接Ｒ２‖Ｒ３を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで暗号化する。ステップＳ９６において、コンテンツプロバイダ２の相互認証部３９は、暗号化した連接Ｒ２‖Ｒ３をＥＭＤサービスセンタ１の相互認証部１７に送信する。

ステップＳ９７において、ＥＭＤサービスセンタ１の相互認証部１７は、暗号化された連接Ｒ２‖Ｒ３を自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ９８において、ＥＭＤサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ８４で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなけば、不適正なプロバイダとして、処理を終了する。

以上のように、ＥＭＤサービスセンタ１の相互認証部１７とコンテンツプロバイダ２の相互認証部３９は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵Ｋｔｅｍｐとして利用される。

（６－２）コンテンツプロバイダからサービスプロバイダへのコンテンツの伝送

次に、図３８のステップＳ１２の処理について説明する。ステップＳ１２にお

いては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ２－１からサービスプロバイダ３－１に供給される処理が行われる。その処理の詳細は、図４３のフローチャートに示されている。すなわち、ステップＳ２０１において、コンテンツプロバイダ２－１のウォータマーク付加部３２（図１１）は、コンテンツサーバ３１からコンテンツＡを読み出し、コンテンツプロバイダ２－１を示す所定のウォータマーク（電子透かし）を挿入し、圧縮部３３に供給する。

ステップＳ２０２において、コンテンツプロバイダ２－１の圧縮部３３は、ウォータマークが挿入されたコンテンツＡをＡＴＲＡＣ２等の所定の方式で圧縮し、暗号化部３４に供給する。ステップＳ２０３において、乱数発生部３５は、コンテンツ鍵ＫｃｏＡとなる乱数を発生させ、暗号化部３４に供給する。

ステップＳ２０４において、コンテンツプロバイダ２－１の暗号化部３４は、ＤＥＳなどの所定の方式で、乱数発生部３５で発生された乱数（コンテンツ鍵ＫｃｏＡ）を使用して、ウォータマークが挿入されて圧縮されたコンテンツＡを暗号化する。次に、ステップＳ２０５において、暗号化部３６は、ＤＥＳなどの所定の方式で、ＥＭＤサービスセンタ１から供給された配送用鍵Ｋｄでコンテンツ鍵ＫｃｏＡを暗号化する。

ステップＳ２０６において、コンテンツプロバイダ２－１のセキュアコンテナ作成部３８は、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびポリシー記憶部３７に記憶されている、コンテンツＡに対応するＵＣＰＡ，Ｂ（図１２）の全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化する。これにより、図１７に示した署名が作成される。

ステップＳ２０７において、コンテンツプロバイダ２－１のセキュアコンテナ作成部３８は、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、ＵＣＰＡ，Ｂ（図１２）、およびステップＳ２０６で生成した署名を含んだ、図１７に示したコンテ

ンツプロバイダセキュアコンテナを作成する。

ステップＳ２０８において、コンテンツプロバイダ２－１の相互認証部３９は、サービスプロバイダ３－１の相互認証部４５（図１９）と相互認証する。この認証処理は、図４０乃至図４２を参照して説明した場合と同様であるので、その説明は省略する。ステップＳ２０９において、コンテンツプロバイダ２－１のセキュアコンテナ作成部３８は、認証局から予め発行された証明書（図１８）を、ステップＳ２０７で作成したコンテンツプロバイダセキュアコンテナに付して、サービスプロバイダ３－１に送信する。

このようにして、コンテンツプロバイダセキュアコンテナが、サービスプロバイダ３－１に供給されたとき、処理は終了し、図３８のステップＳ１３に進む。

（６－３）サービスプロバイダからレシーバへのコンテンツの伝送

ステップＳ１３において、サービスプロバイダセキュアコンテナが、サービスプロバイダ３－１からユーザホームネットワーク５（レシーバ５１）に供給される。この処理の詳細は、図４４のフローチャートに示されている。すなわち、ステップＳ２２１において、サービスプロバイダ３－１の値付け部４２（図１９）は、コンテンツプロバイダ２－１から送信されたコンテンツプロバイダセキュアコンテナに付された証明書（図１８）に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ２－１の公開鍵Ｋｐｃｐを取り出す。証明書の署名の確認は、図４２のステップＳ８３における処理と同様であるので、その説明は省略する。

ステップＳ２２２において、サービスプロバイダ３－１の値付け部４２は、コンテンツプロバイダ２－１から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ２－１の公開鍵Ｋｐｃｐで復号し、得られたハッシュ値が、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびＵＣＰＡ，Ｂの全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値

が一致しない場合（改竄が発見された場合）は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップＳ２２３に進む。

ステップＳ２２３において、サービスプロバイダ３－１の値付け部４２は、コンテンツプロバイダセキュアコンテナから、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、および署名を取り出し、コンテンツサーバ４１に供給する。コンテンツサーバ４１は、それらを記憶する。値付け部４２はまたＵＣＰＡ，Ｂも、コンテンツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部４４に供給する。

ステップＳ２２４において、サービスプロバイダ３－１の値付け部４２は、取り出したＵＣＰＡ，Ｂに基づいて、ＰＴＡ－１，Ａ－２（図２０）、およびＰＴＢ－１，Ｂ－２（図２２）を作成し、セキュアコンテナ作成部４４に供給する。

ステップＳ２２５において、サービスプロバイダ３－１のセキュアコンテナ作成部４４は、コンテンツサーバ４１から読み出したコンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）およびコンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）と、値付け部４２から供給された、ＵＣＰＡ，Ｂ、およびＰＴＡ－１，Ａ－２，Ｂ－１，Ｂ－２、並びにその署名から、図２４に示したサービスプロバイダセキュアコンテナを作成する。

ステップＳ２２６において、サービスプロバイダ３－１の相互認証部４５は、レシーバ５１の相互認証モジュール７１（図２６）と相互認証する。この認証処理は、図４０乃至図４２を参照して説明した場合と同様であるので、その説明を省略する。

ステップＳ２２７において、サービスプロバイダ３－１のセキュアコンテナ作成部４４は、ステップＳ２２５で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ３－１の証明書（図２５）を付して、ユーザホームネットワーク５のレシーバ５１に送信する。

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイダ３－１からレシーバ５１に送信されたとき、処理は終了し、図３８のステップＳ１４に進む。

（６－４）レシーバによるコンテンツの記録処理

ステップＳ１４において、サービスプロバイダ３－１から送信されたサービスプロバイダセキュアコンテナが、ユーザホームネットワーク５のレシーバ５１により受信される。この処理の詳細は、図４５のフローチャートに示されている。すなわち、ステップＳ２４１において、レシーバ５１の相互認証モジュール７１（図２６）は、通信部６１を介して、サービスプロバイダ３－１の相互認証部４５（図１９）と相互認証し、相互認証できたとき、通信部６１は、相互認証したサービスプロパイダ３－１から、サービスプロバイダセキュアコンテナ（図２４）を受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップＳ２４２に進む。

ステップＳ２４２において、レシーバ５１の通信部６１は、ステップＳ２４１で相互認証したサービスプロバイダ３－１から、公開鍵証明書を受信する。

ステップＳ２４３において、レシーバ５１の復号／暗号化モジュール７４は、ステップＳ２４１で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップＳ２４４に進む。

ステップＳ２４４において、レシーバ５１の記憶モジュール７３に記憶されている基準情報５１（図３２）に基づいて、利用条件を満たすＵＣＰと価格条件を満たすＰＴが選択され、表示制御部６７を介して、図示せず表示部に表示される。ユーザＦは、表示されたＵＣＰおよびＰＴの内容を参照して、図示せぬ操作部を操作し、ＵＣＰの１つの利用内容を選択する。これにより、入力制御部６８は、操作部から入力された、ユーザＦの操作に対応する信号をＳＡＭ６２に出力する。

この例の場合、レシーバ５１の基準情報５１の「利用ポイント情報」には、図３３に示したように、コンテンツプロバイダ２－１のコンテンツ利用ポイントが２２２ポイントであるとされてる。すなわち、この基準情報５１によれば、コンテンツＡに対応して設定されたＵＣＰＡ，Ｂのうち、「利用条件１０」の「ユーザ条件１０」が”２００ポイント以上”とされている、ＵＣＰＡが選択される。また、基準情報５１の「決済ユーザ情報」には、ユーザＦは男性とされているので、ＰＴＡ－１（図２０Ａ）の「価格条件１０」に設定された条件を満たす。その結果、ＵＣＰＡに対応して作成されたＰＴＡ－１，ＰＴＡ－２のうち、ＰＴＡ－１が選択される。結局、ＵＣＰＡおよびＰＴＡ－１の内容が、表示部に表示される。また、この例の場合、これにより、ユーザＦが、ＵＣＰＡの利用内容１１（ＰＴＡ－１の価格内容１１）を選択したものとする。

ステップＳ２４５において、レシーバ５１のＳＡＭ６２の課金処理モジュール７２は、ステップＳ２４４で選択された、ＵＣＰＡの「利用内容１１」の内容（ＰＴＡ－１の「価格内容１１」の内容）に基づいて、ＵＣＳＡ（図２８）および課金情報Ａ（図３０）を作成する。すなわち、この場合、コンテンツＡは、料金が２０００円で買い取り再生される。

ステップＳ２４６において、サービスプロバイダセキュアコンテナ（図２４）に含まれる、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、ＵＣＰＡ、ＰＴ－１，Ａ－２、およびコンテンツプロバイダ２の署名が取り出され、ＨＤＤ５２に出力され、記憶される。ステップＳ２４７において、復号／暗号化ユニット７４の復号ユニット９１は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）を、記憶モジュール７３に記憶されている配送用鍵Ｋｄで復号する。

ステップＳ２４８において、復号／暗号化ユニット７４の暗号化ユニット９３は、ステップＳ２４７で復号されたコンテンツ鍵ＫｃｏＡを、記憶モジュール７３に記憶されている保存用鍵Ｋｓａｖｅで暗号化する。

ステップＳ２４９において、ＳＡＭ６２のデータ検査モジュール７５は、ステ

ップＳ２４８で保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵ＫｃｏＡ、およびステップＳ２４５で作成されたＵＣＳＡが対応して記憶される、外部記憶部６３の利用情報記憶部６３Ａ（図２９）の空き領域を有するブロックＢＰを検出する。この例の場合、利用情報記憶部６３Ａのブロック８Ｐ－１が検出される。なお、図２９の利用情報記憶部６３Ａにおいて、そのブロックＢＰ－１の利用情報用メモリ領域ＲＰ－３にコンテンツ鍵ＫｃｏＡおよびＵＣＳＡが記憶されているように示されているが、この例の場合、この時点において、それらは記憶されておらず、ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－３は、空いており、所定の初期情報が記憶されているものとする。

ステップＳ２５０において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２４９で検出したブロックＢＰ－１のデータ（利用情報用メモリ領域ＲＰ－１乃至ＲＰ－Ｎに記憶されている全てのデータ）にハッシュ関数を適用して、ハッシュ値を得る。次に、ステップＳ２５１において、データ検査モジュール７５は、ステップＳ２５０で得られたハッシュ値と、記憶モジュール７３に記憶されているブロックＢＰ－１に対応する検査値ＨＰ－１（図３１）とを比較し、一致するか否かを判定し、一致すると判定した場合、そのブロックＢＰ－１のデータは改竄されていないので、ステップＳ２５２に進む。

ステップＳ２５２において、レシーバ５１のＳＡＭ６２は、利用情報（ステップＳ２４８で、保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵ＫｃｏＡ、およびステップＳ２４５で作成されたＵＣＳＡ（図２８））を、図２９に示すように、利用情報記憶部６３Ａ（外部記憶部６３）のブロックＢＰ－１の利用情報用メモリ領域ＲＰ－３に記憶させる。

ステップＳ２５３において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２５２で利用情報が記憶された利用情報用メモリ領域ＲＰ－３が属する、利用情報記憶部６３Ａのブロック８Ｐ－１のデータにハッシュ関数を適用し、ハッシュ値を算出し、ステップＳ２５４において、記憶モジュール７３に記憶されている検査値ＨＰ－１に上書きする。ステップＳ２５５において、課金処理モ

ジュール７２は、ステップＳ２４５で作成した課金情報Ａを記憶モジュール７３に記憶させ、処理は終了する。

ステップＳ２５１において、算出されたハッシュ値と検査値ＨＰ－１とが一致しないと判定された場合、ブロックＢＰ－１のデータは改竄されているので、手続きは、ステップＳ２５６に進み、データ検査モジュール７５は、外部記憶部６３の利用情報記憶部６３Ａの全てのブロックＢＰを調べたか否かを判定し、外部記憶部６３の全てのブロックＢＰを調べていないと判定した場合、ステップＳ２５７に進み、利用情報記憶部６３Ａの、調べていない（空きを有する他の）ブロックＢＰを検索し、ステップＳ２５０に戻り、それ以降の処理が実行される。

ステップＳ２５６において、外部記憶部６３の利用情報記憶部６３Ａの全てのブロックＢＰが調べられたと判定された場合、利用情報を記憶できるブロックＢＰ（利用情報用メモリ領域ＲＰ）は存在しないので、処理は終了する。

このように、サービスプロバイダセキュアコンテナが、レシーバ５１により受信されると、処理は終了し、図３８のステップＳ１５に進む。

（６－５）コンテンツの再生処理

ステップＳ１５において、供給されたコンテンツＡが、レシーバ５１において利用される。なお、この例の場合、図４５のステップＳ２２４で選択されたＵＣＰＡの利用内容１１によれば、コンテンツＡは、再生して利用される。そこで、ここでは、コンテンツＡの再生処理について説明する。この再生処理の詳細は、図４６のフローチャートに示されている。

ステップＳ２６１において、レシーバ５１のデータ検査モジュール７５は、図４５のステップＳ２５２で、コンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）およびＵＣＳＡが記憶された利用情報用メモリ領域ＲＰ－３が属する、外部記憶部６３の利用情報記憶部６３Ａのブロック ＢＰ－１のデータにハッシュ関数を適用してハッシュ値を算出する。

ステップＳ２６２において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２６１において算出したハッシュ値が、図４５のステップＳ２５３で算

出し、ステップＳ２５４で記憶モジュール７３に記憶させたハッシュ値（検査値ＨＰ－１）と一致するか否かを判定し、一致すると判定した場合、ブロックＢＰ－１のデータは改竄されていないので、ステップＳ２６３に進む。

ステップＳ２６３において、ＵＣＳＡ（図２８）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツＡが利用可能か否かが判定される。例えば、「利用内容」の「形式」が、”期間制限再生”とされているＵＣＳにおいては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。すなわち、現在時刻が、その範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされているＵＣＳにおいては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が０回でないとき、対応するコンテンツの利用が可能であると判定され、一方、利用可能回数が０回であるとき、利用不可と判定される。

なお、ＵＣＳＡの「利用内容」の「形式」は、”買い取り再生”とされているので、この場合、コンテンツＡは、買い取られ、制限なしに再生される。すなわち、ＵＣＳＡの「利用内容」の「パラメータ」には、コンテンツが利用可能であることを示す情報が設定されている。そのため、この例の場合では、ステップＳ２６３において、コンテンツＡが利用可能であると判定され、ステップＳ２６４に進む。

ステップＳ２６４において、レシーバ５１の課金モジュール７２は、ＵＣＳＡを更新する。ＵＣＳＡには、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、その「パラメータ」に記憶されている、再生可能回数が１つだけデクリメントされる。

次に、ステップＳ２６５において、レシーバ５１のＳＡＭ６２は、ステップＳ

２６４で更新されたＵＣＳＡ（この例の場合には、実際は、更新されていない）を、外部記憶部６３の利用情報記憶部６３ＡのブロックＢＰ－１の利用情報用メモリ領域ＲＰ－３に記憶させる。ステップＳ２６６において、データ検査モジュール７５は、ステップＳ２６５でＵＣＳＡが記憶された、外部記憶部６３の利用情報記憶部６３ＡのブロックＢＰ－１のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール７３に記憶されている検査値ＨＰ－１に上書きする。

ステップＳ２６７において、ＳＡＭ６２の相互認証モジュール７１と、伸張部６４の相互認証モジュール１０１は、相互認証し、ＳＡＭ６２および伸張部６４は、一時鍵Ｋｔｅｍｐを共有する。この認証処理は、図４０乃至図４２を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、Ｒ３、またはその組み合わせが、一時鍵Ｋｔｅｍｐとして用いられる。

ステップＳ２６８において、復号／暗号化モジュール７４の復号ユニット９１は、図４５のステップＳ２５２で外部記憶部６３の利用情報記憶部６３ＡのブロックＢＰ－１（利用情報用メモリ領域ＲＰ－３）に記憶されたコンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）を、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。

次に、ステップＳ２６９において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵ＫｃｏＡを一時鍵Ｋｔｅｍｐで暗号化する。ステップＳ２７０において、ＳＡＭ６２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵ＫｃｏＡを伸張部６４に送信する。

ステップＳ２７１において、伸張部６４の復号モジュール１０２は、コンテンツ鍵ＫｃｏＡを一時鍵Ｋｔｅｍｐで復号する。ステップＳ２７２において、伸張部６４は、インタフェース６６を介して、ＨＤＤ５２に記録されたコンテンツＡ（コンテンツ鍵Ｋｃｏで暗号化されている）を受け取る。ステップＳ２７３において、伸張部６４の復号モジュール１０３は、コンテンツＡ（コンテンツ鍵Ｋｃ

ｏで暗号化されている）をコンテンツ鍵ＫｃｏＡで復号する。

ステップＳ２７４において、伸張部６４の伸張モジュール１０４は、復号されたコンテンツＡをＡＴＲＡＣ２などの所定の方式で伸張する。ステップＳ２７５において、伸張部６４のウォータマーク付加モジュール１０５は、伸張されたコンテンツＡにレシーバ５１を特定する所定のウォータマーク（電子透かし）を挿入する。ステップＳ２７６において、コンテンツＡは、図示せぬスピーカなどに出力され、処理は終了する。

ステップＳ２６２において、ステップＳ２６１において算出されたハッシュ値が、レシーバ５１の記憶モジュール７３に記憶されたハッシュ値と一致しないと判定された場合、またはステップＳ２６３において、コンテンツが利用不可と判定された場合、ステップＳ２７７において、ＳＡＭ６２は、表示制御部６７を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

このようにして、レシーバ５１において、コンテンツＡが再生（利用）されたとき、処理は終了し、図３８の処理も終了する。

（６－６）決済処理

次に、レシーバ５１の課金が決済される場合の処理手順を、図４７のフローチャートを参照して説明する。なお、この処理は、計上された課金が所定の上限額（正式登録時の上限額または仮登録時の上限額）を越えた場合、または配送用鍵Ｋｄのバージョンが古くなり、例えば、図４５のステップＳ２４７で、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）を復号することができなくなった場合（サービスプロバイダセキュアコンテナを受信することができなくなった場合）に開始される。

ステップＳ３０１において、レシーバ５１とＥＭＤサービスセンタ１との相互認証が行われる。この相互認証は、図４０乃至図４２を参照して説明した場合と同様の処理であるので、その説明は省略する。

次に、ステップＳ３０２において、レシーバ５１のＳＡＭ６２は、ＥＭＤサー

ビスセンタ１のユーザ管理部１８（図３）に証明書を送信する。ステップＳ３０３において、レシーバ５１のＳＡＭ６２は、記憶モジュール７３に記憶されている課金情報を、ステップＳ３０１で、ＥＭＤサービスセンタ１と共有した一時鍵Ｋｔｅｍｐで暗号化し、配送用鍵Ｋｄのバージョン、ＨＤＤ５２に記憶されてる、対応するＵＣＰとＰＴ、並びに登録リストとともに、ＥＭＤサービスセンタ１に送信する。

ステップＳ３０４において、ＥＭＤサービスセンタ１のユーザ管理部１８は、ステップＳ３０３で、レシーバ５１から送信された情報を受信し、復号した後、ＥＭＤサービスセンタ１のユーザ管理部１８が、登録リストの「状態フラグ」に”停止”が設定されるべき不正行為がレシーバ５１において存在するか否かを確認する。

ステップＳ３０５において、ＥＭＤサービスセンタ１の課金請求部１９は、ステップＳ３０３で受信された課金情報を解析し、ユーザ（例えば、ユーザＦ）の支払い金額を算出する処理等を行う。次に、ステップＳ３０６において、ユーザ管理部１８は、ステップＳ３０５における処理により、決済が成功したか否かを確認する。

次に、ステップＳ３０７において、ＥＭＤサービスセンタ１のユーザ管理部１８は、ステップＳ３０４における確認結果、およびステップＳ３０６における確認結果に基づいて、レシーバ５１の登録条件を設定し、それに署名を付して、レシーバ５１の登録リストを作成する。

例えば、ステップＳ３０４で、不正行為が確認された場合、「状態フラグ」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、ＥＭＤシステムからのサービスを一切受けることができなくなる。また、ステップＳ３０６で、決済が成功しなかったことが確認された場合、「状態フラグ」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

次に、ステップＳ３０８に進み、ＥＭＤサービスセンタ１のユーザ管理部１８

は、最新バージョンの配送用鍵Ｋｄ（３ヶ月分の最新バージョンの配送用鍵Ｋｄ）およびステップＳ３０７で作成された登録リストを、一時鍵Ｋｔｅｍｐで暗号化し、レシーバ５１に送信する。なお、登録リストには、署名が付されているので、暗号化しなくてもよい。

ステップＳ３０９において、レシーバ５１のＳＡＭ６２は、ＥＭＤサービスセンタ１から送信された配送用鍵Ｋｄおよび登録リスト情報を、通信部６１を介して受信し、復号した後、配送用鍵Ｋｄを記憶モジュール７３に記憶させ、登録リストをＨＤＤ５２に記憶させる。このとき、記憶モジュール７３に記憶されていた課金情報は消去され、登録リストおよび配送用鍵Ｋｄが更新される。

（６－７）管理移動の設定

次に、レシーバ５１からレシーバ２０１に、コンテンツＡが管理移動される場合の処理手順を、図４８のフローチャートを参照して説明する。

ステップＳ４０１において、レシーバ５１とレシーバ２０１との間で、相互認証が行われる。この相互認証は、図４０乃至図４２を参照して説明した同様であるので、その説明は省略する。

次に、ステップＳ４０２において、レシーバ５１（管理移動元の機器）のＳＡＭ６２およびレシーバ２０１（管理移動先の機器のＳＡＭ）のＳＡＭ２１２のそれぞれは、各自が保持する登録リストを参照し、コンテンツの管理移動が可能であるか否かを確認する。具体的には、管理移動元の機器のＳＡＭ（レシーバ５１のＳＡＭ６２）は、自分の登録リストに、管理移動先の機器（レシーバ２０１）の登録条件が設定されているか否かを確認し、それが設定されている場合、コンテンツの管理移動が可能であると判定する。同様に、管理移動先の機器のＳＡＭ（レシーバ２０１のＳＡＭ２１２）も、自分の登録リストに、管理移動元の機器（レシーバ５１）の登録条件が設定されているか否かを確認し、それが設定されている場合、コンテンツの管理移動が可能であると判定する。いずれか一方においても、コンテンツの管理移動が可能でないと判定された場合、処理は終了するが、この例の場合、それぞれの登録条件は、それぞれの登録リストに設定されて

いるので、両者において、コンテンツの管理移動が可能であると判定され、ステップＳ４０３に進む。

次に、ステップＳ４０３において、レシーバ２０１のデータ検査モジュール２２５は、後述するステップＳ４１４で受信する移動情報（コンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）、コンテンツＡのＩＤ、およびＳＡＭ６２のＩＤ）を記憶する、外部記憶部２１３の移動情報記憶部２１３Ａ（図３６）のブロックＢＭを検出する。この例の場合、ステップＳ４０３において、ブロックＢＭ－１が検出される。なお、図３６の利用情報記憶部２１３Ａにおいて、そのブロックＢＭ－１の移動情報用メモリ領域ＲＭ－１には、コンテンツ鍵ＫｃｏＡ、コンテンツＡのＩＤ、およびＳＡＭ６２のＩＤが記憶されているように示されているが、この例の場合、この時点において、その移動情報用メモリ領域ＲＭ－１は、空いているものとする。

ステップＳ４０４において、レシーバ２０１のデータ検査モジュール２２５は、ステップＳ４０３で検出したブロックＢＭ－１のデータが改竄されているか否かを判定する。具体的には、データ検査モジュール２２５は、ブロックＢＭ－１に記憶されているデータにハッシュ関数を適用してハッシュ値を算出する。そしてデータ検査モジュール２２５は、算出したハッシュ値と、記憶モジュール２２３に記憶される、ブロックＢＭ－１に対応する検査値ＨＭ－１が一致するか否かを判定し、一致していると判定した場合、すなわち、ブロックＢＭ－１が改竄されていない場合、ステップＳ４０５に進む。

ステップＳ４０５において、レシーバ２０１のＳＡＭ２１２は、コンテンツの管理移動が可能であることを示す信号を通信部２１５を介して、レシーバ５１に送信する。

ステップＳ４０６において、レシーバ５１が、レシーバ２０１から、コンテンツの管理移動が可能であることを示す信号を受信すると、レシーバ５１のデータ検査モジュール７５は、管理移動されるコンテンツＡに対応するコンテンツ鍵ＫｃｏＡが記憶されている、外部記憶部６３の利用情報記憶部６３Ａ（図２９）の

ブロックＢＰ－１を検出する。

ステップＳ４０７において、レシーバ５１のデータ検査モジュール７５は、ステップＳ４０６で検出したブロックＢＰ－１のデータが改竄されているか否かを判定する。具体的には、データ検査モジュール７５は、ブロックＢＰ－１に記憶されているデータの全てにハッシュ関数を適用してハッシュ値を算出する。そしてデータ検査モジュール７５は、算出したハッシュ値が、記憶モジュール７３に記憶されている、ブロックＢＰ－１に対応する検査値ＨＰ－１（図４５のステップＳ２５３で算出され、ステップＳ２５４で記憶されたハッシュ値）と一致するか否かを判定し、一致すると判定した場合、すなわち、ブロックＢＰ－１のデータが改竄されていない場合、ステップＳ４０８に進む。

ステップＳ４０８において、レシーバ５１のＳＡＭ６２は、ステップＳ４０６で検出された、外部記憶部６３の利用情報記憶部６３のブロックＢＰ－１（利用情報用メモリ領域ＲＰ－３）に記憶されているＵＣＳＡ（図２８）の「利用内容」の「形式」を参照し、コンテンツの利用形式が”買い取り再生”であるか否かを判定する。ＵＣＳＡの場合のように、その「利用内容」の「形式」が、”買い取り再生”とされているとき、コンテンツの利用形式が”買い取り再生”であると判定され、ステップＳ４０９に進む。

ステップＳ４０９において、レシーバ５１のＳＡＭ６２は、ＵＣＳＡの「利用内容」の「管理移動状態情報」に設定されている管理移動先の機器のＩＤが、自分自身のＩＤとされているか否か、すなわち、コンテンツが管理移動されているか否かを判定し、コンテンツが管理移動されていないと判定した場合、ステップＳ４１０に進む。

ステップＳ４１０において、レシーバ５１のＳＡＭ６２は、今回のコンテンツＡの管理移動先の機器であるレシーバ２０１のＳＡＭ２１２のＩＤを、ＵＣＳＡの「利用内容」の「管理移動状態情報」に管理移動先の機器のＩＤとして設定する。次に、ステップＳ４１１において、レシーバ５１のデータ検査モジュール７５は、ステップＳ４１０で、「利用内容」の「管理移動状態情報」の内容が変更

（管理移動先のＩＤが、ＳＡＭ６２のＩＤからＳＡＭ２１２のＩＤに変更）されたＵＣＳＡが記憶されているブロックＢＰ－１のデータにハッシュ関数を適用しハッシュ値を算出し、それを、ステップＳ４１２において、記憶モジュール７３に記憶されている、ブロックＢＰ－１に対応するハッシュ値ＨＰ－１に上書きする。

次に、ステップＳ４１３において、レシーバ５１のＳＡＭ６２は、外部記憶部６３の利用情報記憶部６３Ａのブロック ＢＰ－１（利用情報用メモリ領域ＲＰ－３）に記憶されているコンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）を保存用鍵Ｋｓａｖｅで復号し、ステップＳ４０１でレシーバ２０１と共有した一時鍵Ｋｔｅｍｐで暗号化した後、自分自身のＩＤ（ＳＡＭ６２のＩＤ）およびＵＣＳＡの「コンテンツのＩＤ」に設定されているコンテンツＡのＩＤとともに、レシーバ２０１に送信する。なお、この処理が実行されるタイミングで、ＨＤＤ５２に記憶されているコンテンツＡは、レシーバ２０１に送信される。

ステップＳ４１４において、レシーバ５１から送信されてきたコンテンツ鍵ＫｏｃＡ（一時鍵Ｋｔｅｍｐで暗号化されている）、ＳＡＭ６２のＩＤ、およびコンテンツＡのＩＤがレシーバ２０１により受信されると、ステップＳ４１５において、レシーバ２０１のＳＡＭ２１２は、受信されたコンテンツ鍵ＫｃｏＡ（一時鍵Ｋｔｅｍｐで暗号化されている）を一時鍵Ｋｔｅｍｐで復号した後、自分自身が保持している保存用鍵Ｋｓａｖｅで再度暗号化して、それを、同様にＳＡＭ６２のＩＤ、コンテンツＡのＩＤ、および自分自身のＩＤ（ＳＡＭ２１２のＩＤ）とともに、ステップＳ４０３で検出した、外部記憶部２１３の移動情報記憶部２１３Ａのブロック ＢＰ－１の移動情報用メモリ領域ＲＭ－１に、図３６で示したように記憶させる。

次に、ステップＳ４１６において、レシーバ２０１のＳＡＭ２１２は、ステップＳ４１５で移動情報が記憶された移動情報記憶部２１３Ａのブロック ＢＭ－１のデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール２２３

に記憶されている検査値ＨＭ－１に上書きする。

ステップＳ４１７において、レシーバ５１から供給されたコンテンツＡがＨＤＤ２０２に記憶される。

ステップＳ４０４で外部記憶部２１３の移動情報記憶部２１３Ａのブロック ＢＭ－１のデータが、またはステップＳ４０７で外部記憶部６３の利用情報記憶部６３Ａのブロック ＢＰ－１のデータが改竄されていると判定された場合、処理は終了する。すなわち、移動情報が記憶されるメモリ領域がまたは、利用情報が改竄されている場合（正確には、改竄されている恐れがある場合）、コンテンツの管理移動は行われない。

ステップＳ４０７で、コンテンツＡの利用形式が”買い取り”ではないと判定された場合、またはステップＳ４０８で、コンテンツＡが管理移動されていると判定された場合も、処理は終了する。すなわち、コンテンツを買い取って再生する利用形式においてのみ、コンテンツの管理移動が行われる（許可されている）。また、コンテンツが管理移動されている間は、さらに、そのコンテンツを管理移動することはできない（許可されていない）。

（６－８）管理移動の解除

次に、上述した処理により、レシーバ２０１にコンテンツＡが管理移動されている状態において、今度は、レシーバ５１が、コンテンツＡを戻す（管理移動を解除する）場合の処理手順を、図４９のフローチャートを参照して説明する。

ステップＳ４３１において、レシーバ５１とレシーバ２０１との間で、相互認証が行われる。この相互認証は、図４０乃至図４２を参照して説明した場合と同様であるので、その説明は省略する。次に、ステップＳ４３２において、レシーバ５１（管理移動元の機器）のＳＡＭ６２およびレシーバ２０１（管理移動先の機器のＳＡＭ）のＳＡＭ２１２のそれぞれは、各自が保持する登録リストを参照し、管理移動の解除が可能であるかを確認する。なお、ここでの具体的な処理は、図４８のステップＳ４０２における場合と同様であるので、その説明は省略する。

ステップＳ４３３において、レシーバ５１のデータ検査モジュール７５は、管理移動されているコンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）に対応するコンテンツ鍵ＫｃｏＡが記憶されている外部記憶部６３の利用情報記憶部６３Ａ（図２９）のブロックＢＰを検出する。この例の場合、ブロックＢＰ－１が検出される。

次に、ステップＳ４３４において、レシーバ５１のデータ検査モジュール７５は、ステップＳ４３３で検出したブロックＢＰ－１のデータが改竄されているか否かを判定する。ここでの具体的な処理は、図４８のステップＳ４０７における場合と同様であるので、その説明は省略する。

ステップＳ４３４で、外部記憶部６３の利用情報記憶部６３Ａのブロック ＢＰ－１のデータが改竄されていないと判定された場合、ステップＳ４３５に進み、レシーバ５１のＳＡＭ６２は、外部記憶部６３の利用情報記憶部６３Ａのブロックブロック ＢＰ－１に記憶されているＵＣＳＡ（図２８）から、コンテンツＡのＩＤおよびＳＡＭ６２のＩＤを読み出し、それらを、管理移動の解除を要求する所定の信号（以下、管理移動解除要求信号と称する）とともに、レシーバ２０１に送信する。

ステップＳ４３６において、レシーバ５１から送信されてきた、コンテンツＡのＩＤ、ＳＡＭ６２のＩＤ、および管理移動解除要求信号が受信されると、ステップＳ４３７において、レシーバ２０１のＳＡＭ２１２は、受信されたコンテンツＡのＩＤが記憶されている、外部記憶部２１３の移動情報記憶部２１３Ａのブロック ＢＭを検出する。この例の場合、ブロックＢＭ－１が検出される。

ステップＳ４３８において、レシーバ２０１のＳＡＭ２１２は、外部記憶部２１３の移動情報記憶部２１３Ａのブロック ＢＭ－１（移動情報用メモリ領域ＲＭ－１）に、ステップＳ４３６で受信されたＳＡＭ６２のＩＤが記憶されているか否かを判定し、記憶されていると判定した場合、ステップＳ４３９に進む。この例の場合、ブロックＢＭ－１の移動情報用メモリ領域ＲＭ－１には、ＳＡＭ６２のＩＤが記憶されているので、ステップＳ４３９に進む。

ステップＳ４３９において、レシーバ２０１のＳＡＭ２１２は、ＳＡＭ６２のＩＤが記憶されてるブロックＢＭ－１が改竄されているか否かを判定する。ここでの具体的な処理は、図４８のステップＳ４０４における場合と同様であるので、その説明は省略する。ステップＳ４３９において、ブロックＢＭ－１が改竄されていないと判定された場合、ステップＳ４４０に進む。

ステップＳ４４０において、レシーバ２０１のＳＡＭ２１２は、外部記憶部２１３の移動情報記憶部２１３Ａのブロック ＢＭ－１（移動情報用メモリ領域ＲＭ－１）に、ステップＳ４３６で受信されたコンテンツのＩＤが記憶されているか否かを判定し、記憶されていると判定した場合、ステップＳ４４１に進む。この例の場合、ブロックＢＭ－１の移動情報用メモリ領域ＲＭ－１には、コンテンツＡのＩＤが記憶されているので、ステップＳ４４１に進む。

ステップＳ４４１において、レシーバ２０１のＳＡＭ２１２は、外部記憶部２１３の移動情報記憶部２１３Ａのブロック ＢＭ－１（移動情報用メモリ領域ＲＭ－１）に記憶されている移動情報を削除する。これにより、ブロックＢＭ－１の移動情報用メモリ領域ＲＭ－１には、所定の初期情報が記憶される。なお、この処理が実行されるタイミングで、ＨＤＤ２０２に記憶されているコンテンツＡも削除される。

次に、ステップＳ４４２において、レシーバ２０１のデータ検査モジュール２２５は、ステップＳ４４１で移動情報が削除された移動情報用メモリ領域ＲＭ－１が属するブロックＢＭ－１のデータにハッシュ関数を適用してハッシュ値を算出し、それを、記憶モジュール２２３に記憶されている、ブロックＢＭ－１に対応するハッシュ値ＨＭ－１に上書きする。

ステップＳ４４３において、レシーバ２０１のＳＡＭ２１２は、コンテンツの管理移動が解除されたことを示す信号（以下、管理移動解除信号と称する）を、レシーバ５１に送信する。

ステップＳ４４４おいて、レシーバ２０１からの管理移動解除信号が受信されると、レシーバ５１のＳＡＭ６２は、自分自身のＩＤを、ＵＣＳＡの「利用内容」

の「管理移動状態情報」に、管理移動先の機器のＩＤとして記憶させる（管理移動元の機器のＩＤは、ＳＡＭ６２のＩＤとされている）。

次に、ステップＳ４４５において、レシーバ５１のデータ検査モジュール７５は、ステップＳ４４４で、「利用内容」の管理移動状態情報の内容が変更（管理移動先のＩＤが、ＳＡＭ２１２のＩＤからＳＡＭ６２のＩＤに変更）されたＵＣＳＡが記憶されているブロックＢＰ－１のデータにハッシュ関数を適用してハッシュ値を算出し、それを、ステップＳ４４６において、記憶モジュール７３に記憶されている、ブロックＢＰ－１に対応する検査値ＨＰ－１に上書きする。

以上のようにして、コンテンツの管理移動が解除されるとき、管理移動先の機器である、レシーバ２０１から移動情報が削除されるようにしたので、レシーバ２０１においてコンテンツＡは利用されないようになる。またこのとき、ＵＣＳＡの「利用内容」の「管理移動状態情報」に、管理移動元の機器のＳＡＭのＩＤ（レシーバ５１のＳＡＭ６２）のＩＤが、管理移動先の機器のＩＤとしても設定されるようにしたので、レシーバ５１は、コンテンツＡの管理移動を行うことができるようになる。

なお、以上においては、コンテンツの利用形式が”買い取り再生”である場合にのみ管理移動が可能となる場合を例として説明したが、利用形式が”期間制限再生”である場合においても管理移動が可能となるようにすることもできる。

また、以上においては、管理移動が解除される場合、レシーバ５１がレシーバ２０１に管理移動解除要求信号を送信する場合（レシーバ５１が管理移動の解除を要求する場合）を例として説明したが、レシーバ２０１が管理移動の解除を要求することもできる。

さらに、以上においては、ＳＡＭ６２の公開鍵ＫｐｕおよびＳＡＭ６２の証明書がレシーバ５１の記憶モジュール７３が記憶されているものとしたが、ＨＤＤ５２に記憶させておくこともできる。同様に、ＳＡＭ２１２の公開鍵ＫｐｕおよびＳＡＭ２１２の証明書も、ＨＤＤ２０２に記憶させておくこともできる。

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動

画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

また、共通鍵暗号は、ブロック暗号であるＤＥＳを使用して説明したが、ＮＴＴ（商標）が提案するＦＥＡＬ、ＩＤＥＡ（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ａｌｇｏｒｉｔｈｍ）、または１ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

さらに、コンテンツおよびコンテンツ鍵Ｋｃｏの暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、ＣＤ－ＲＯＭ、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

上述した本発明の実施の形態のレシーバにおいては、移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および価値情報を復号するのに必要な鍵を含む移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更し、所定の制御信号に対する応答信号が受信されたとき、移動状態情報の内容を、価値情報の移動が行われていないことを示すものに変更するようにしたので、著作権の保護を確保しながら、価値情報の移動を行うことができる。

また、本発明の実施の形態のレシーバにおいては、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信し、所定の制御信号を受信したとき、記憶された移動情報を削除するようにしたので、著作権の保護を確保しながら、移動された価値情報を利用することができ

る。

産業上の利用の可能性

本発明は、音楽データ、動画像データ、静止画像データ、文書データ、プログラムデータなどの情報を暗号化し、配信する情報処理システムに適応できる。

請 求 の 範 囲

1．他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置において、

上記価値情報を復号するのに必要な鍵、上記価値情報の使用条件、および上記価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶手段と、

上記記憶手段により記憶されている上記利用情報に含まれる上記使用条件が所定の条件で、かつ、上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていないことを示しているとき、上記価値情報、および上記利用情報に含まれる上記鍵を含む所定の移動情報を上記他の情報処理装置に供給する供給手段と、

上記供給手段により、上記価値情報、および上記移動情報が上記他の情報処理装置に供給されたとき、上記移動状態情報の内容を、上記価値情報の移動が行われていることを示すものに変更する第１の変更手段と、

上記記憶手段により記憶されている上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていることを示しており、上記情報処理装置への上記価値情報の移動を解除するとき、上記他の情報処理装置に所定の制御信号を送信する送信手段と、

上記他の情報処理装置から、上記送信手段により送信された上記制御信号に対する応答信号を受信したとき、上記移動状態情報の内容を、上記価値情報の移動が行われていないことを示すものに変更する第２の変更手段と

を具備する情報処理装置。

2．上記記憶手段は、所定のメモリ領域に分割されている複数のブロックにより構成され、上記利用情報を、上記所定のメモリ領域に記憶し、

上記記憶手段を構成する上記ブロックに記憶されている複数の上記利用情報の

全体にハッシュ関数を適用し、ハッシュ値を算出する算出手段と、

ハッシュ値を記憶するハッシュ値記憶手段と、

上記算出手段により算出された上記ハッシュ値と、上記ハッシュ値記憶手段に記憶されている所定のハッシュ値を比較し、比較結果に基づいて、上記記憶手段が改竄されたか否かを判定する判定手段と、

上記判定手段による判定結果に基づいて、上記供給手段による供給を制御する制御手段と

をさらに具備する請求の範囲第１項に記載の情報処理装置。

３．他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置の情報処理方法において、

上記価値情報を復号するのに必要な鍵、上記価値情報の使用条件、および上記価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、

上記記憶ステップで記憶された上記利用情報に含まれる上記使用条件が所定の条件で、かつ、上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていないことを示しているとき、上記価値情報、および上記利用情報に含まれる上記鍵を含む所定の移動情報を上記他の情報処理装置に供給する供給ステップと、

上記供給ステップで、上記価値情報、および上記移動情報が上記他の情報処理装置に供給されたとき、上記移動状態情報の内容を、上記価値情報の移動が行われていることを示すものに変更する第１の変更ステップと、

上記記憶ステップで記憶されている上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていることを示しており、上記情報処理装置への上記価値情報の移動を解除するとき、上記他の情報処理装置に所定の制御信号を送信する送信ステップと、

上記他の情報処理装置から、上記送信ステップで送信された上記制御信号に対

する応答信号を受信したとき、上記移動状態情報の内容を、上記価値情報の移動が行われていないことを示すものに変更する第２の変更ステップと

を具備する情報処理方法。

４．他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置に、

上記価値情報を復号するのに必要な鍵、上記価値情報の使用条件、および上記価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、

上記記憶ステップで記憶された上記利用情報に含まれる上記使用条件が所定の条件で、かつ、上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていないことを示しているとき、上記価値情報、および上記利用情報に含まれる上記鍵を含む所定の移動情報を上記他の情報処理装置に供給する供給ステップと、

上記供給ステップで、上記価値情報、および上記移動情報が上記他の情報処理装置に供給されたとき、上記移動状態情報の内容を、上記価値情報の移動が行われていることを示すものに変更する第１の変更ステップと、

上記記憶ステップで記憶されている上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていることを示しており、上記他の情報処理装置への上記価値情報の移動を解除するとき、上記他の情報処理装置に所定の制御信号を送信する送信ステップと、

上記他の情報処理装置から、上記送信ステップで送信された上記制御信号に対する応答信号を受信したとき、上記移動状態情報の内容を、上記価値情報の移動が行われていないことを示すものに変更する第２の変更ステップと

を具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供する提供媒体。

5．他の情報処理装置に接続され、暗号化された上記価値情報を復号し、利用する情報処理装置において、

上記他の情報処理装置から供給される上記価値情報、および上記価値情報を復号するのに必要な鍵を含む移動情報を受信する受信手段と、

上記受信手段により受信された上記移動情報を記憶する記憶手段と、

上記他の情報処理装置から、所定の制御信号を受信したとき、上記記憶手段に記憶されている上記移動情報を削除する削除手段と、

上記削除手段により、上記移動情報が削除されたとき、所定の応答信号を送信する送信手段と

を具備する情報処理装置。

6．上記記憶手段は、所定のメモリ領域に分割されている複数のブロックにより構成され、上記移動情報を、上記所定のメモリ領域に記憶するし、

上記記憶手段の上記ブロックごとに記憶されている複数の上記移動情報の全体にハッシュ関数を適用し、ハッシュ値を算出する算出手段と、

ハッシュ値を記憶するハッシュ値記憶手段と、

上記算出手段により算出された上記ハッシュ値と、上記ハッシュ値記憶手段に記憶されている所定のハッシュ値を比較し、比較結果に基づいて、上記記憶手段が改竄されたか否かを判定する判定手段と、

上記判定手段による判定結果に基づいて、上記受信手段による受信を制御する制御手段と

をさらに具備する請求の範囲第5項に記載の情報処理装置。

7．他の情報処理装置に接続され、暗号化された上記価値情報を復号し、利用する情報処理装置の情報処理方法において、

上記他の情報処理装置から供給される上記価値情報、および上記価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、

上記受信ステップで受信された上記移動情報を記憶する記憶ステップと、

上記他の情報処理装置から、所定の制御信号を受信したとき、上記記憶ステップで記憶された上記移動情報を削除する削除ステップと、

上記削除ステップで、上記移動情報が削除されたとき、所定の応答信号を送信する送信ステップと

を具備する情報処理方法。

8．他の情報処理装置に接続され、暗号化された上記価値情報を復号し、利用する情報処理装置に、

上記他の情報処理装置から供給される上記価値情報、および上記価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、

上記受信ステップで受信された上記移動情報を記憶する記憶ステップと、

上記他の情報処理装置から、所定の制御信号を受信したとき、上記記憶ステップで記憶された上記移動情報を削除する削除ステップと、

上記削除ステップで、上記移動情報が削除されたとき、所定の応答信号を送信する送信ステップと

を具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供する提供媒体。

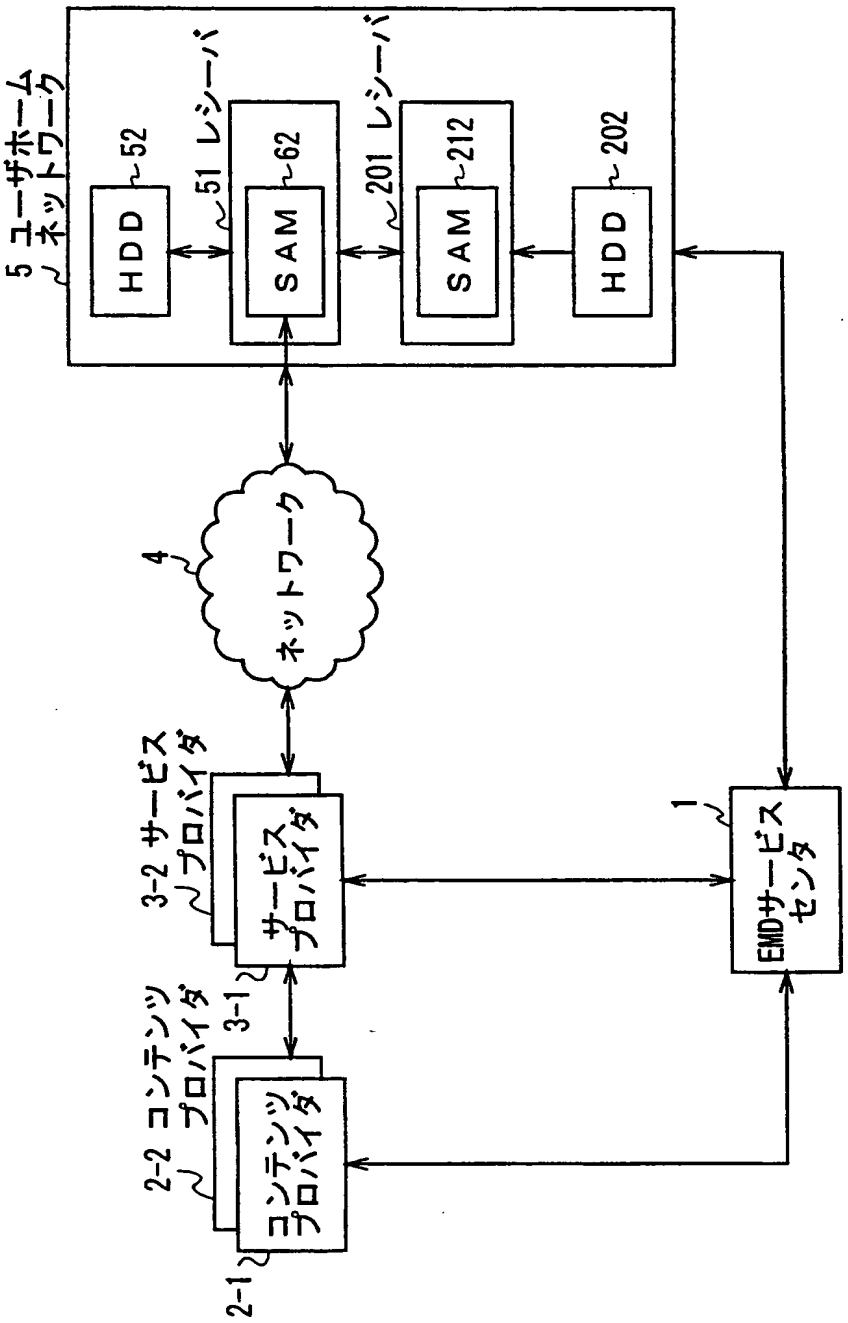

5 ユーザホーム ネットワーク
HDD
52
51 レシーバ
SAM
62
201 レシーバ
SAM
212
HDD
202
4
ネットワーク
3-2 サービス プロバイダ
サービス プロバイダ
3-1
2-2 コンテンツ プロバイダ
コンテンツ プロバイダ
2-1
1
EMDサービス センタ

図 1

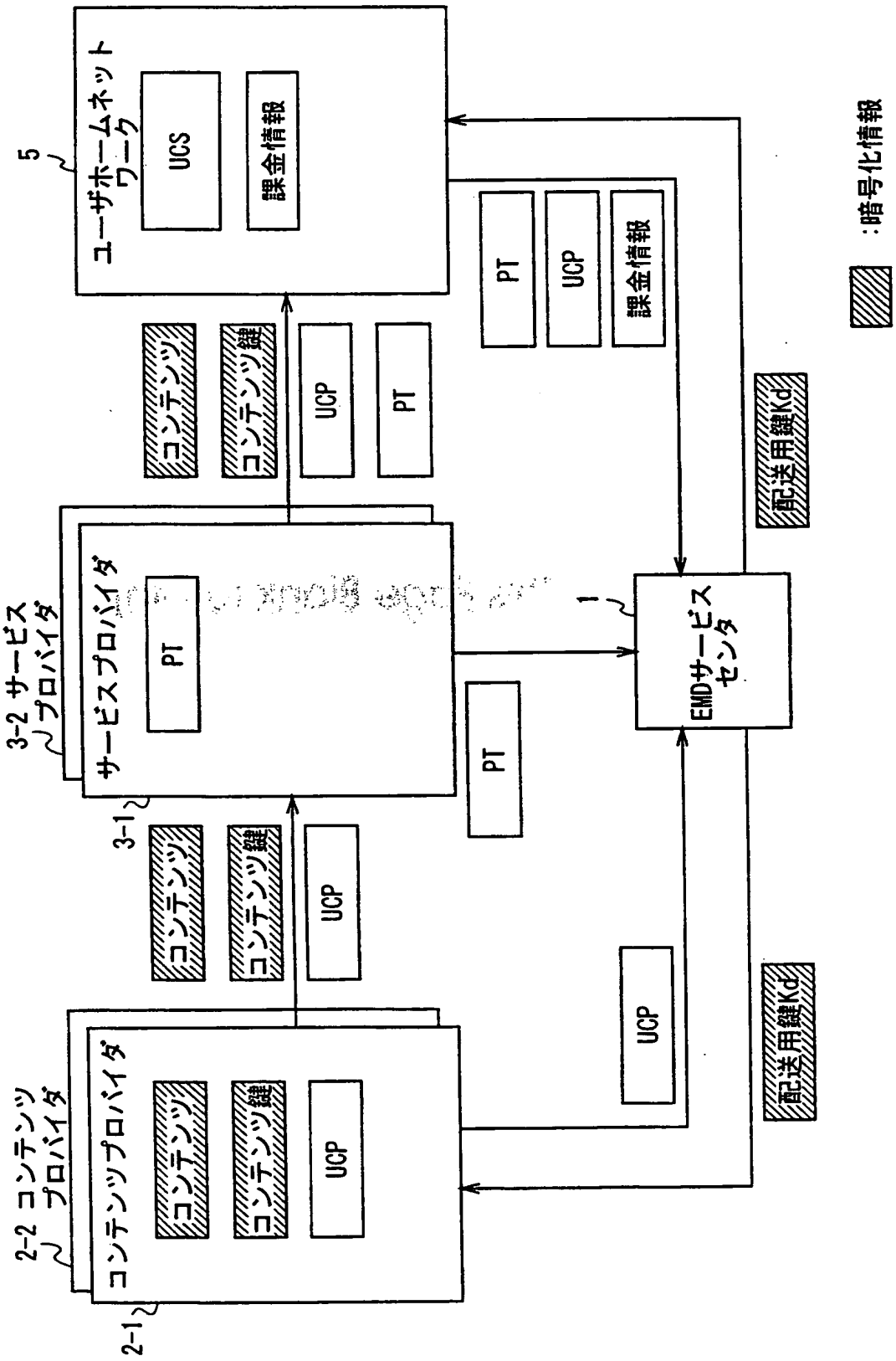
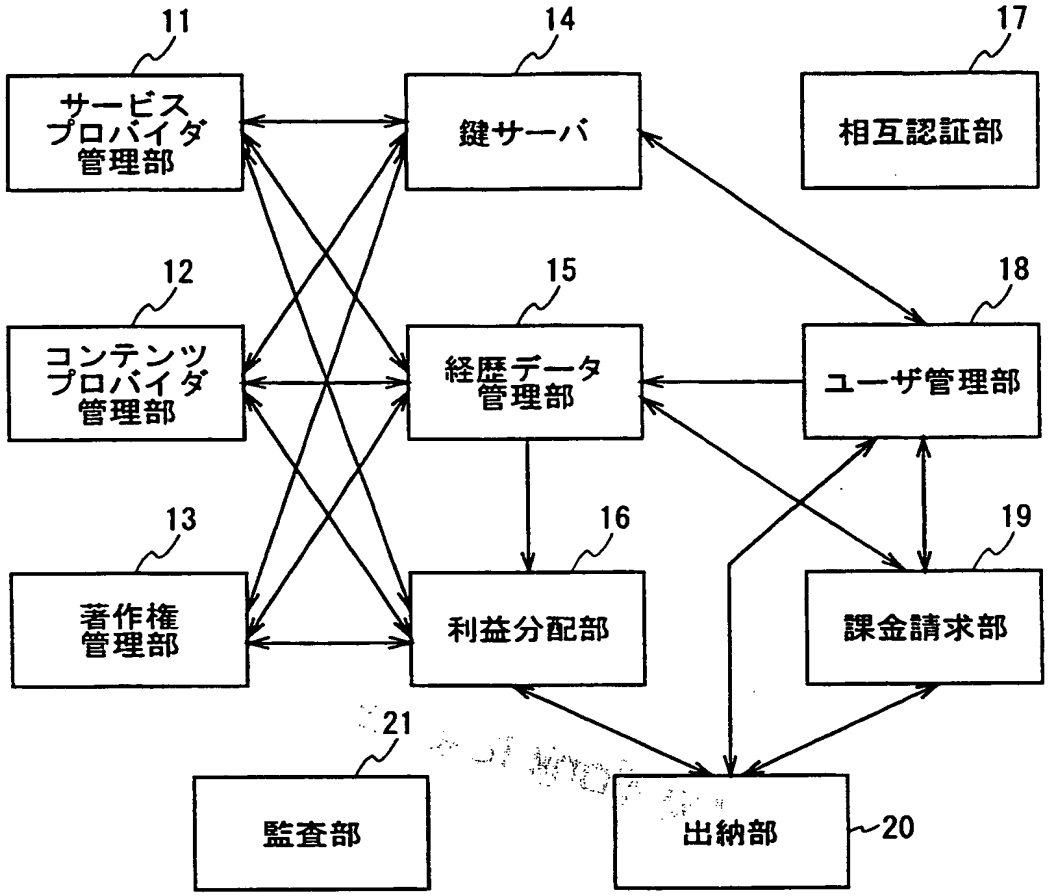

5
ユーザホームネットワーク
UCS
課金情報
PT
UCP
課金情報
コンテンツ
コンテンツ鍵
UCP
PT
配送用鍵Kd
3-2 サービスプロバイダ
サービスプロバイダ
PT
1
EMDサービスセンタ
PT
3-1
コンテンツ
コンテンツ鍵
UCP
UCP
配送用鍵Kd
2-2 コンテンツプロバイダ
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
UCP
2-1
:暗号化情報

図2



EMDサービスセンタ 1

図３

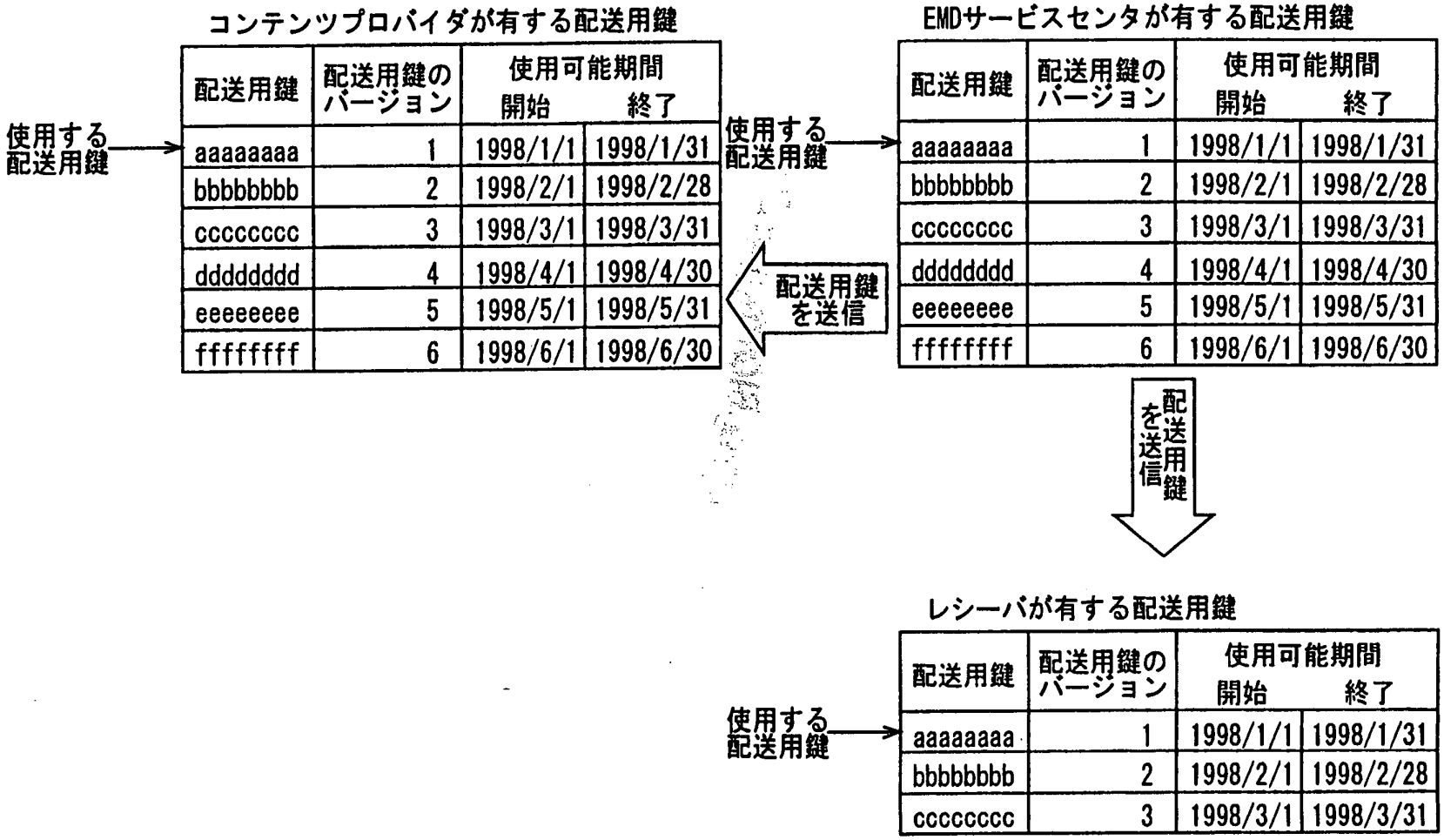

コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間
開始
終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間
開始
終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間
開始
終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
使用する配送用鍵

図4

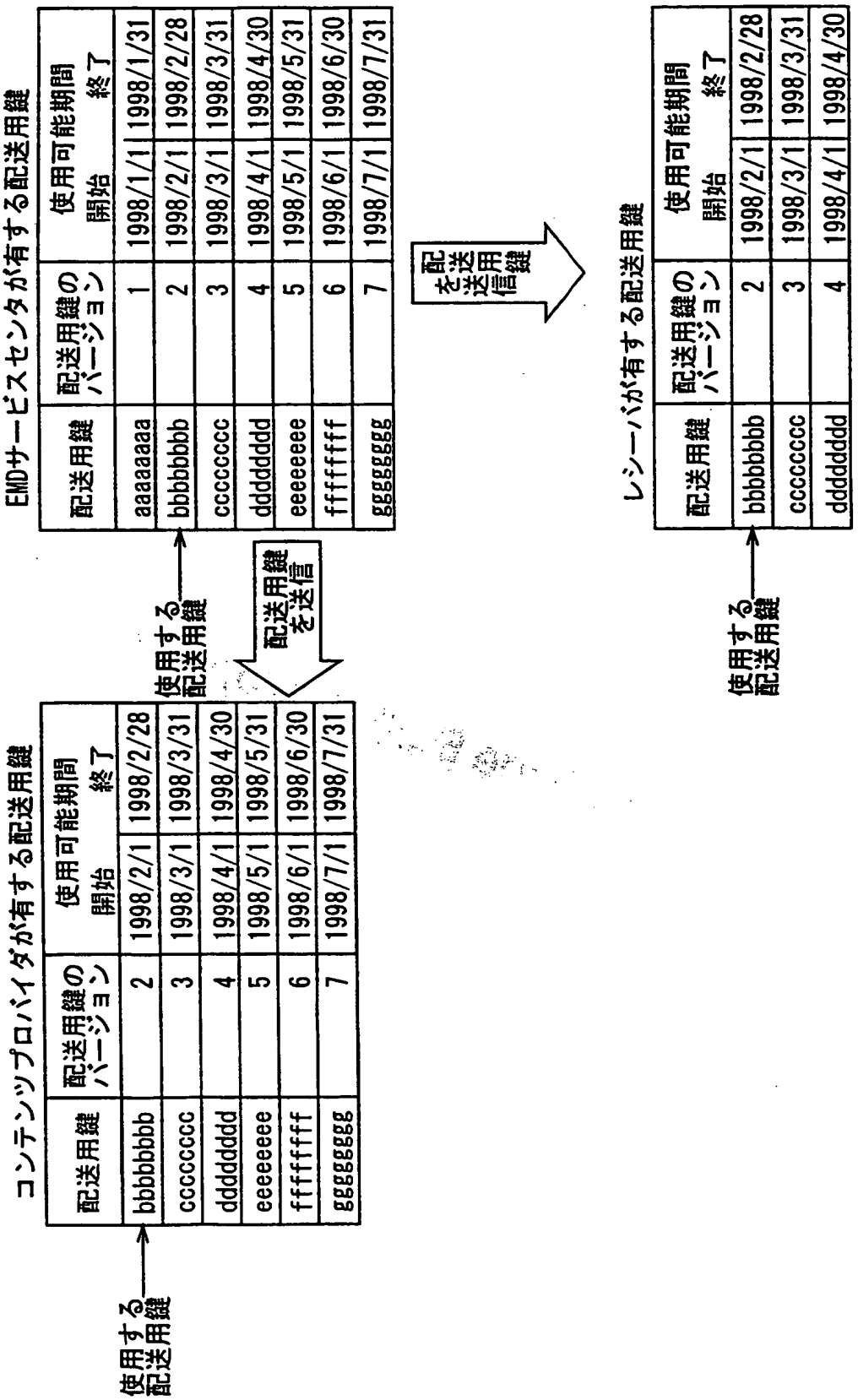

コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
配を送用信鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
使用する配送用鍵

図5

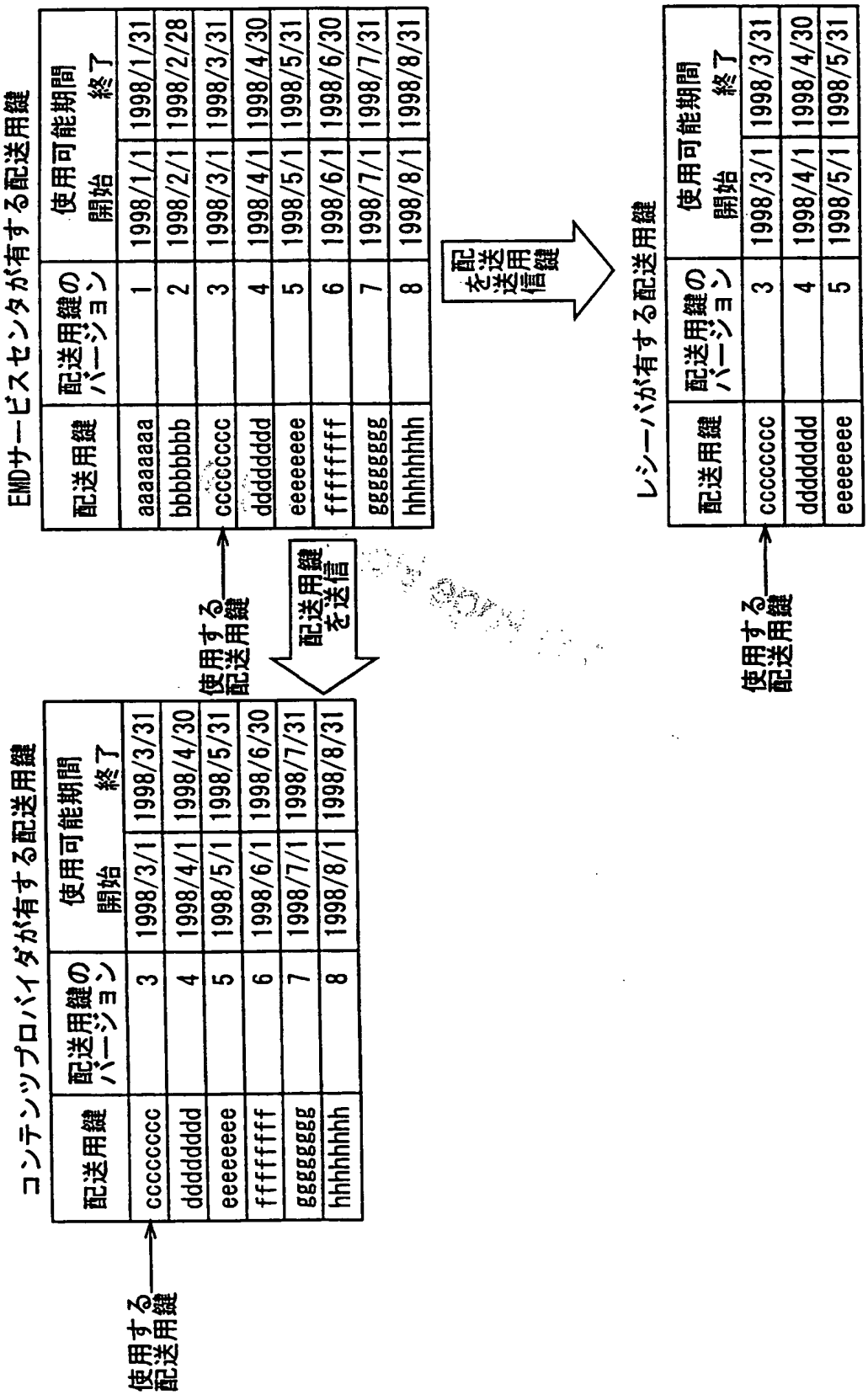

コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
使用する配送用鍵
配送用鍵を送信
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31

図6

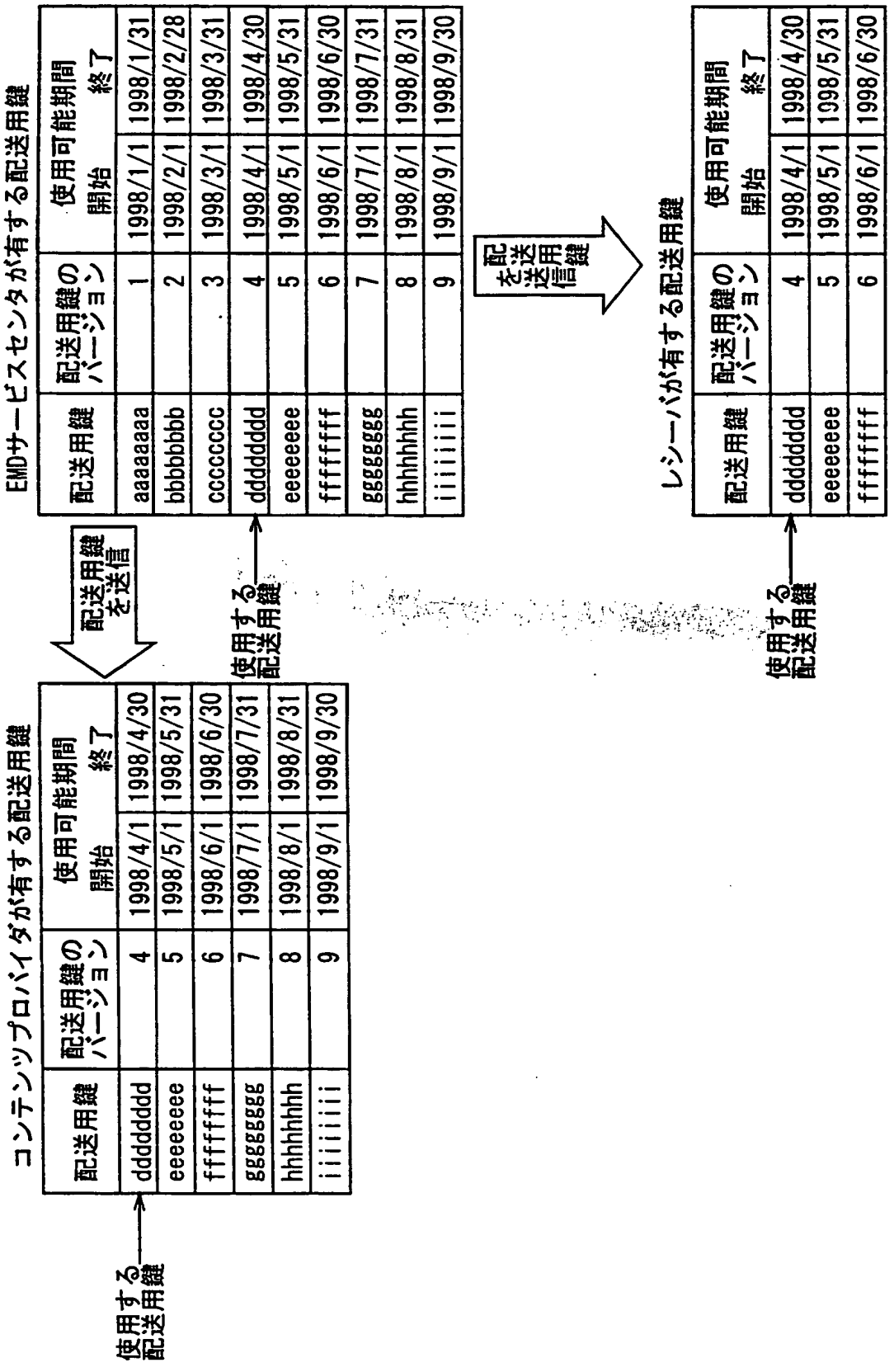

コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
使用する配送用鍵
配送用鍵を送信
使用する配送用鍵
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
配送用鍵を送信
使用する配送用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵

図 7

配送用鍵	配送用鍵のバージョン	使用可能期間 開始	終了
aaaaaaaaa	1	1998/1/1	1998/1/31

仮配送用鍵Kd

図8

SAMのID		SAM62のID	SAM212のID
機器番号		ﾚｼｰﾊﾞ51の機器番号(100番)	ﾚｼｰﾊﾞ201の機器番号(100番)
決済ID		ユーザFの決済ID	ユーザAの決済ID
決済ユーザ情報	氏名	ユーザFの氏名	ユーザAの氏名
	住所	ユーザFの住所	ユーザAの住所
	電話番号	ユーザFの電話番号	ユーザAの電話番号
	決済機関情報	ユーザFの決済情報	ユーザAの決済情報
	生年月日	ユーザFの生年月日	ユーザAの生年月日
	年齢	ユーザFの年齢	ユーザAの年齢(35才)
	性別	ユーザFの性別(男)	ユーザAの性別(男)
	ユーザのID	ユーザFのID	ユーザAのID
	パスワード	ユーザFのパスワード	ユーザAのパスワード
従属ユーザ情報	氏名		
	住所		
	電話番号		
	生年月日		
	性別		
	ユーザのID		
	パスワード		
利用ﾎﾟｲﾝﾄ情報		ﾚｼｰﾊﾞ51の利用ﾎﾟｲﾝﾄ情報	ﾚｼｰﾊﾞ201の利用ﾎﾟｲﾝﾄ情報

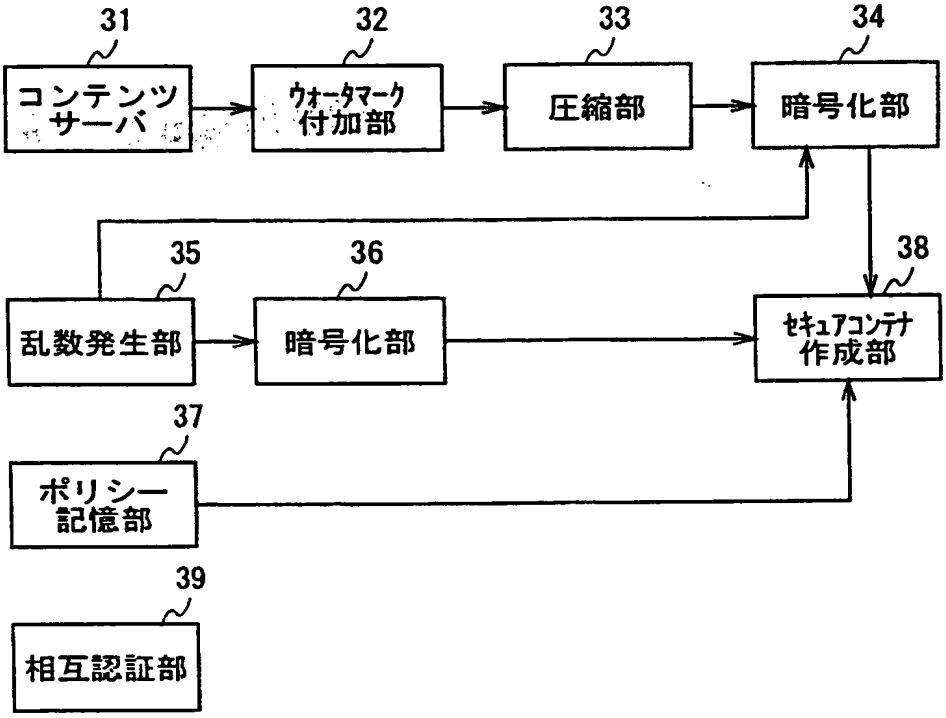
システム登録情報

図9

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	222ポイント
	コンテンツプロバイダ2-2	123ポイント
	サービスプロバイダ3-1	345ポイント
	サービスプロバイダ3-2	0ポイント

利用ポイント情報

図１０



コンテンツプロバイダ 2-1

図１１

A

コンテンツのID	コンテンツAのID	
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	
UCPのID	UCPAのID	
UCPの有効期限	UCPAの有効期限	
利用条件 10	ﾕｰｻﾞ条件10	200ﾎﾟｲﾝﾄ以上
	機器条件10	条件なし
利用内容 11	ID 11	利用内容11のID
	形式11	買い取り再生
	ﾊﾟﾗﾒｰﾀ11	××××
	管理移動許可情報11	可
利用内容 12	ID 12	利用内容12のID
	形式12	第1世代複製
	ﾊﾟﾗﾒｰﾀ12	××××
	管理移動許可情報12	不可
利用内容 13	ID 13	利用内容13のID
	形式13	期間制限再生
	ﾊﾟﾗﾒｰﾀ13	××××
	管理移動許可情報13	不可
利用内容 14	ID 14	利用内容14のID
	形式14	Pay Per Copy 5
	ﾊﾟﾗﾒｰﾀ14	複製5回
	管理移動許可情報14	不可

UCPA

B

コンテンツのID		コンテンツAのID
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID		ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID
UCPのID		UCPBのID
UCPの有効期限		UCPBの有効期限
利用条件 20	ﾕｰｻﾞ条件20	200ﾎﾟｲﾝﾄより少ない
	機器条件20	条件なし
利用内容 21	ID 21	利用内容21のID
	形式21	Pay Per Play 4
	ﾊﾟﾗﾒｰﾀ21	再生4回
	管理移動許可情報21	不可
利用内容 22	ID 22	利用内容22のID
	形式22	Pay Per Copy 2
	ﾊﾟﾗﾒｰﾀ22	複製2回
	管理移動許可情報22	不可

UCPB

図１２

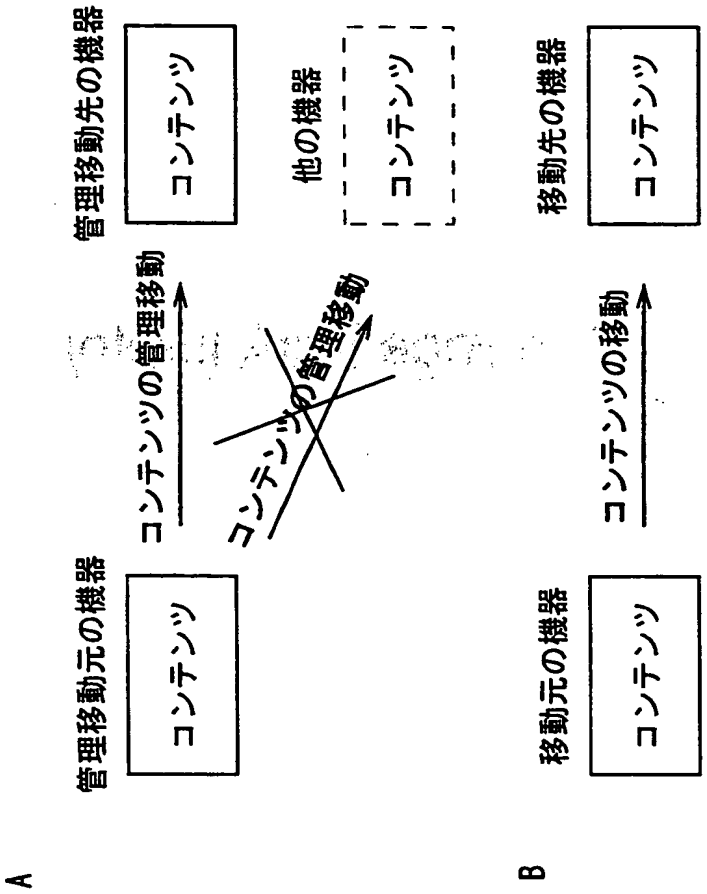

A
管理移動元の機器
コンテンツ
コンテンツの管理移動
管理移動先の機器
コンテンツ
他の機器
コンテンツ
コンテンツの管理移動
B
移動元の機器
コンテンツ
コンテンツの移動
移動先の機器
コンテンツ

図１３

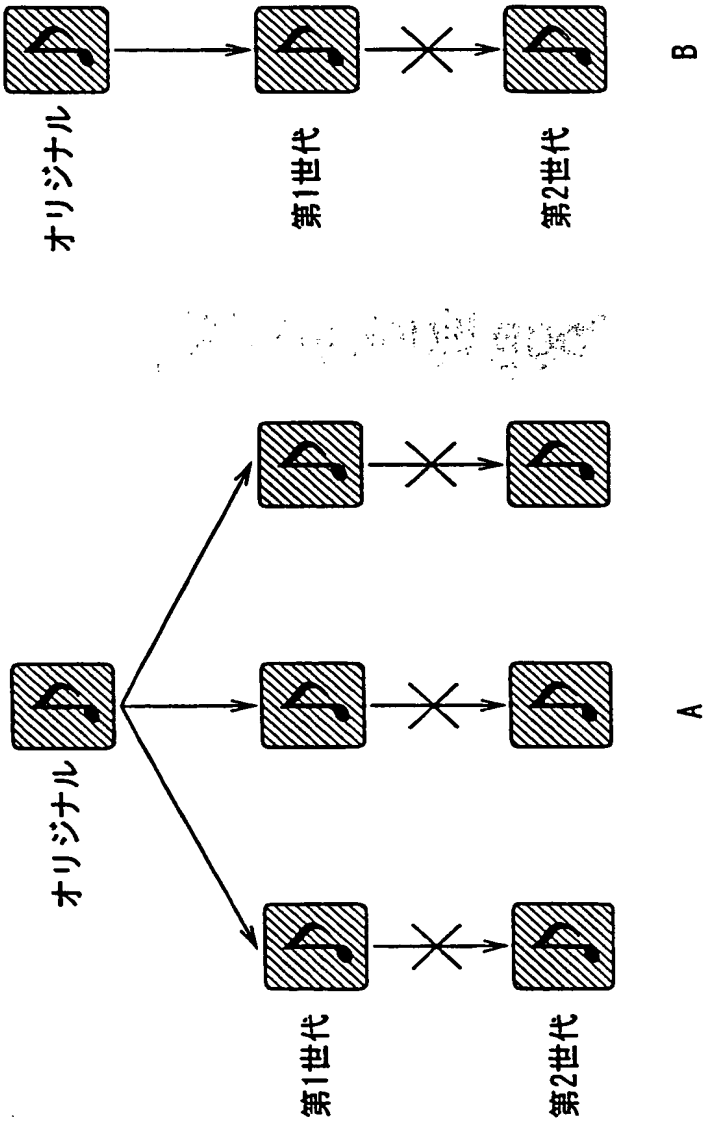


図１４

A

サービスコード	意味
0000h	条件なし
0001h乃至00FFh	機器に関し条件有り
0100h乃至01FFh	性別条件あり
0200h乃至02FFh	年令条件あり
0300h乃至7FFFh	その他の条件あり
8000h乃至FFFFh	利用ポイントに関し条件有り

B

コンディションコード	意味
00h	無条件
01h	＝
02h	≠
03h	＜(より小さい)
04h	＞(より大きい)
05h	≦(以下)
06h	≧(以上)
07h乃至FFh	空き

図１５

A

ユーザ条件 10	サービスコード	バリューコード	コンディションコード
	80×× h	0000C8h	06h
機器条件 10	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

UCPAの利用条件 10

B

ユーザ条件 20	サービスコード	バリューコード	コンディションコード
	80×× h	0000C8h	03h
機器条件 20	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

UCPBの利用条件 20

図１６

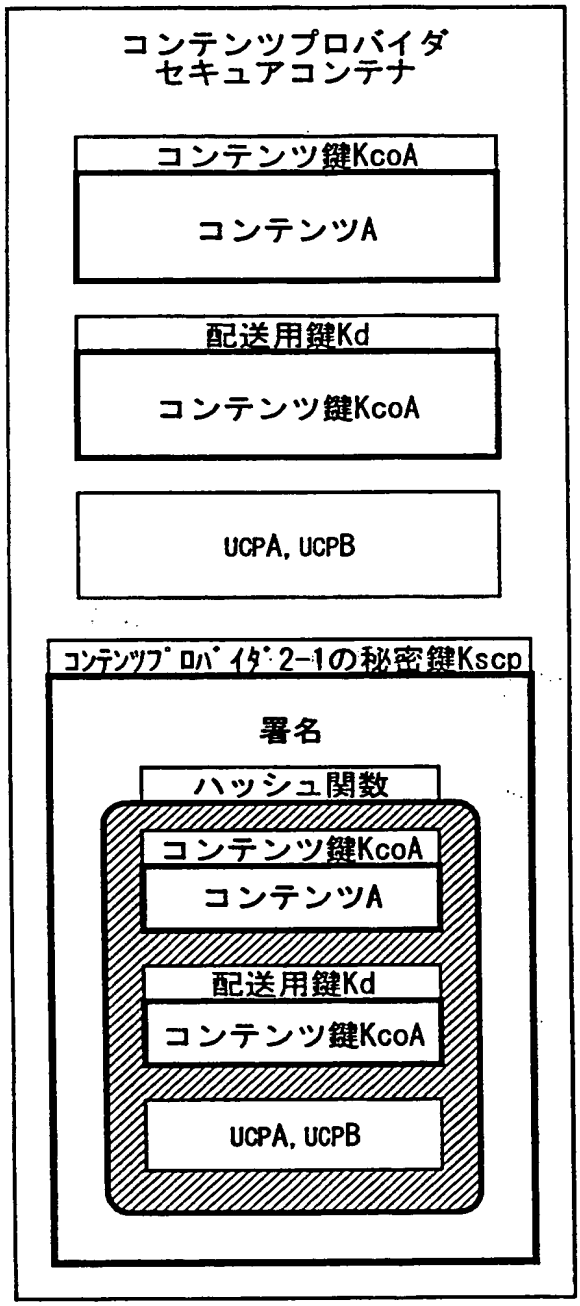

コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵KcoA
コンテンツA
配送用鍵Kd
コンテンツ鍵KcoA
UCPA, UCPB
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1の秘密鍵Kscp
署名
ハッシュ関数
コンテンツ鍵KcoA
コンテンツA
配送用鍵Kd
コンテンツ鍵KcoA
UCPA, UCPB

図１７

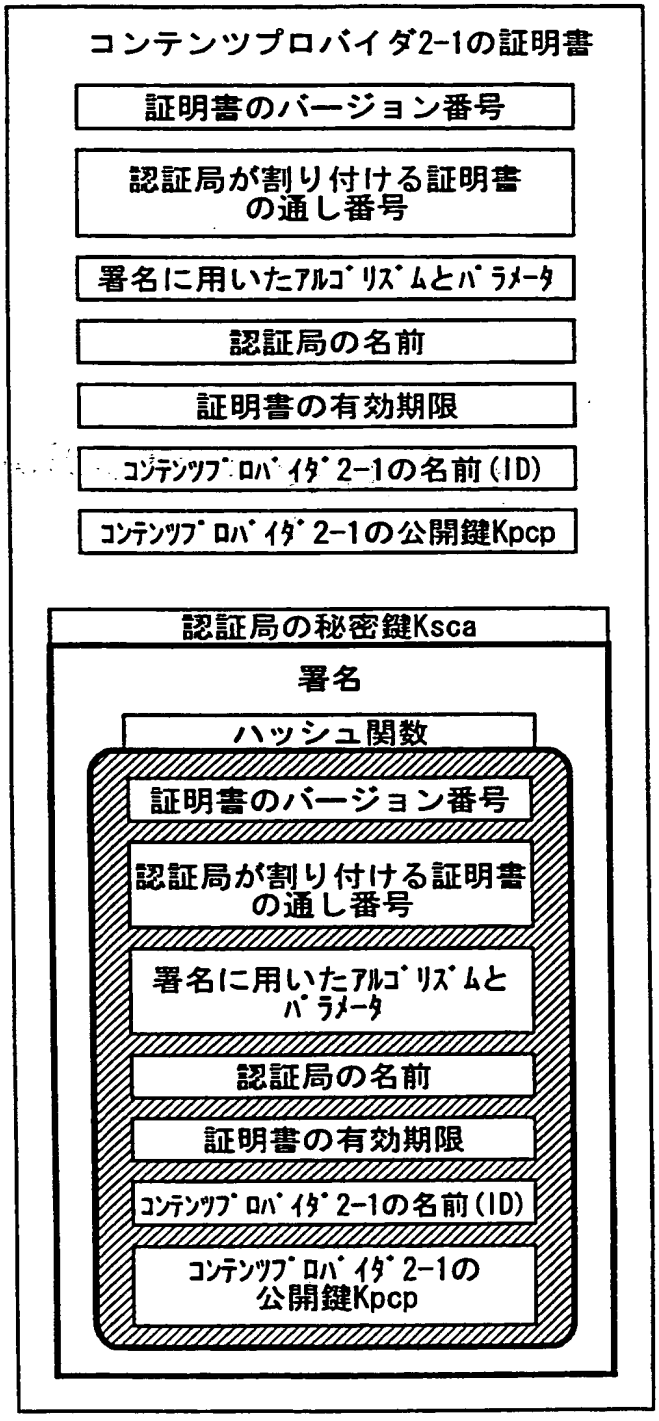
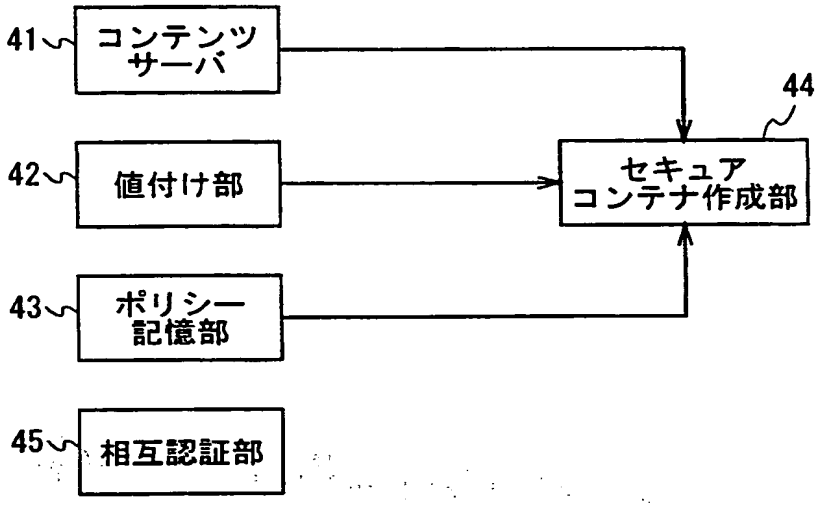

コンテンツプロバイダ2-1の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1の名前(ID)
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1の公開鍵Kpcp
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1の名前(ID)
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1の公開鍵Kpcp

図１８



サービスプロバイダ 3-1

図１９

A

コンテンツのID	コンテンツAのID	
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	
UCPのID	UCPAのID	
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID	ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID	
PTのID	PTA-1のID	
PTの有効期限	PTA-1の有効期限	
価格条件 10	ユーザ条件 10	男性
	機器条件 10	条件なし
価格内容 11	2000円	
価格内容 12	600円	
価格内容 13	100円	
価格内容 14	300円	

PTA-1

B

コンテンツのID	コンテンツAのID	
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	
UCPのID	UCPAのID	
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID	ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID	
PTのID	PTA-2のID	
PTの有効期限	PTA-2の有効期限	
価格条件 20	ユーザ条件 20	女性
	機器条件 20	条件なし
価格内容 21	1000円	
価格内容 22	300円	
価格内容 23	50円	
価格内容 24	150円	

PTA-2

図２０

A

ユーザ条件 10	サービスコード	バリューコード	コンディションコード
	01××h	000000h	01h
機器条件 10	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-1の価格条件 10

B

ユーザ条件 20	サービスコード	バリューコード	コンディションコード
	01××h	000001h	01h
機器条件 20	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-2の価格条件 20

図２１

コンテンツのID	コンテンツAのID	
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	
UCPのID	UCPBのID	
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID	ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID	
PTのID	PTB-1のID	
PTの有効期限	PTB-1の有効期限	
価格条件 30	ユーザ条件 30	条件なし
	機器条件 30	従機器
価格内容 31	100円	
価格内容 32	300円	

PTB-1

A

コンテンツのID	コンテンツAのID	
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	
UCPのID	UCPBのID	
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID	ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID	
PTのID	PTB-2のID	
PTの有効期限	PTB-2の有効期限	
価格条件 40	ユーザ条件 40	条件なし
	機器条件 40	主機器
価格内容 41	50円	
価格内容 42	150円	

PTB-2

B

図２２

A

ユーザ条件 30	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 30	サービスコード	バリューコード	コンディションコード
	00××h	000064h	03h

PTB-1の価格条件 30

B

ユーザ条件 40	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 40	サービスコード	バリューコード	コンディションコード
	00××h	000064h	06h

PTB-2の価格条件 40

図２３

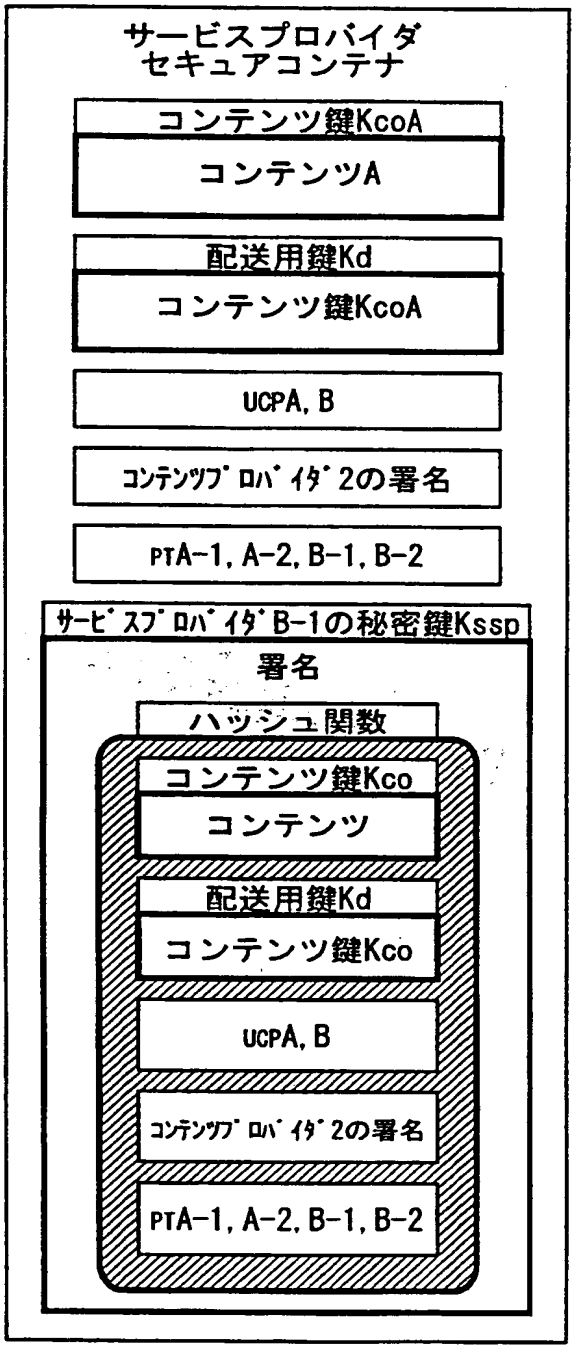

サービスプロバイダ
セキュアコンテナ
コンテンツ鍵KcoA
コンテンツA
配送用鍵Kd
コンテンツ鍵KcoA
UCPA, B
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2の署名
PTA-1, A-2, B-1, B-2
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞB-1の秘密鍵Kssp
署名
ハッシュ関数
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
UCPA, B
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2の署名
PTA-1, A-2, B-1, B-2

図２４

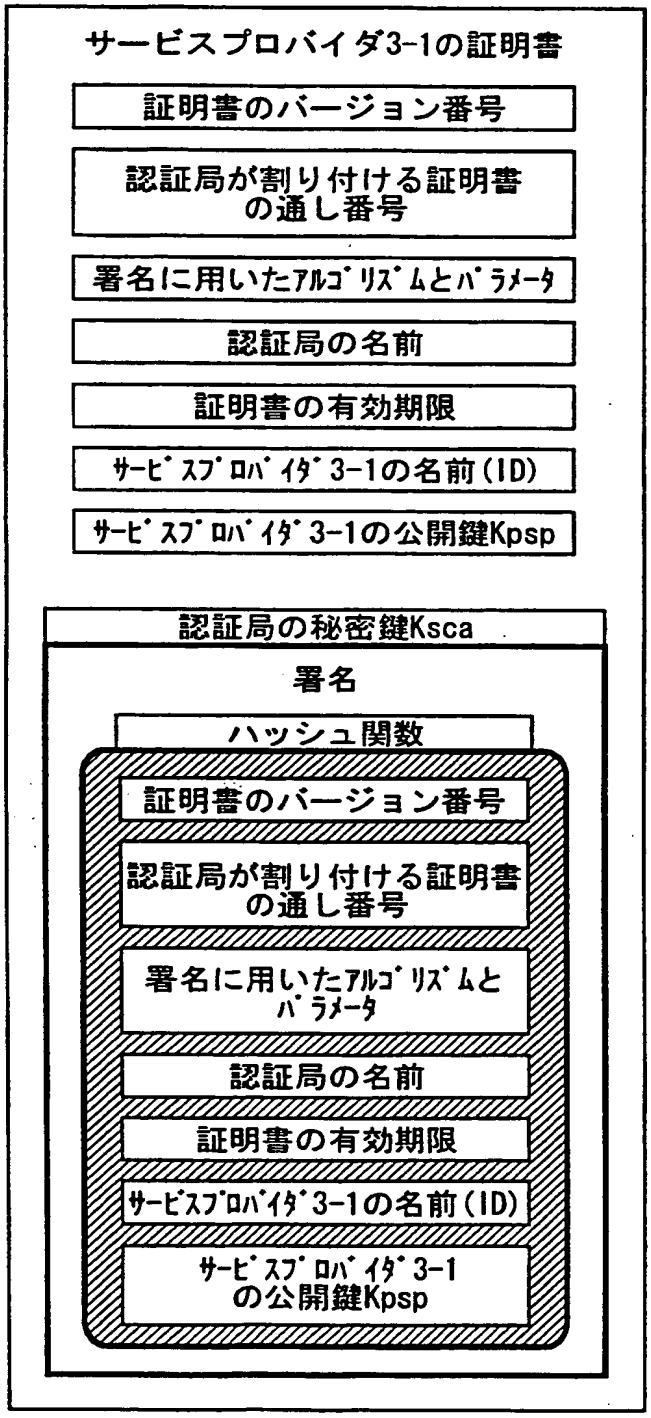

サービスプロバイダ3-1の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1の名前(ID)
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1の公開鍵Kpsp
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1の名前(ID)
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1の公開鍵Kpsp

図２５

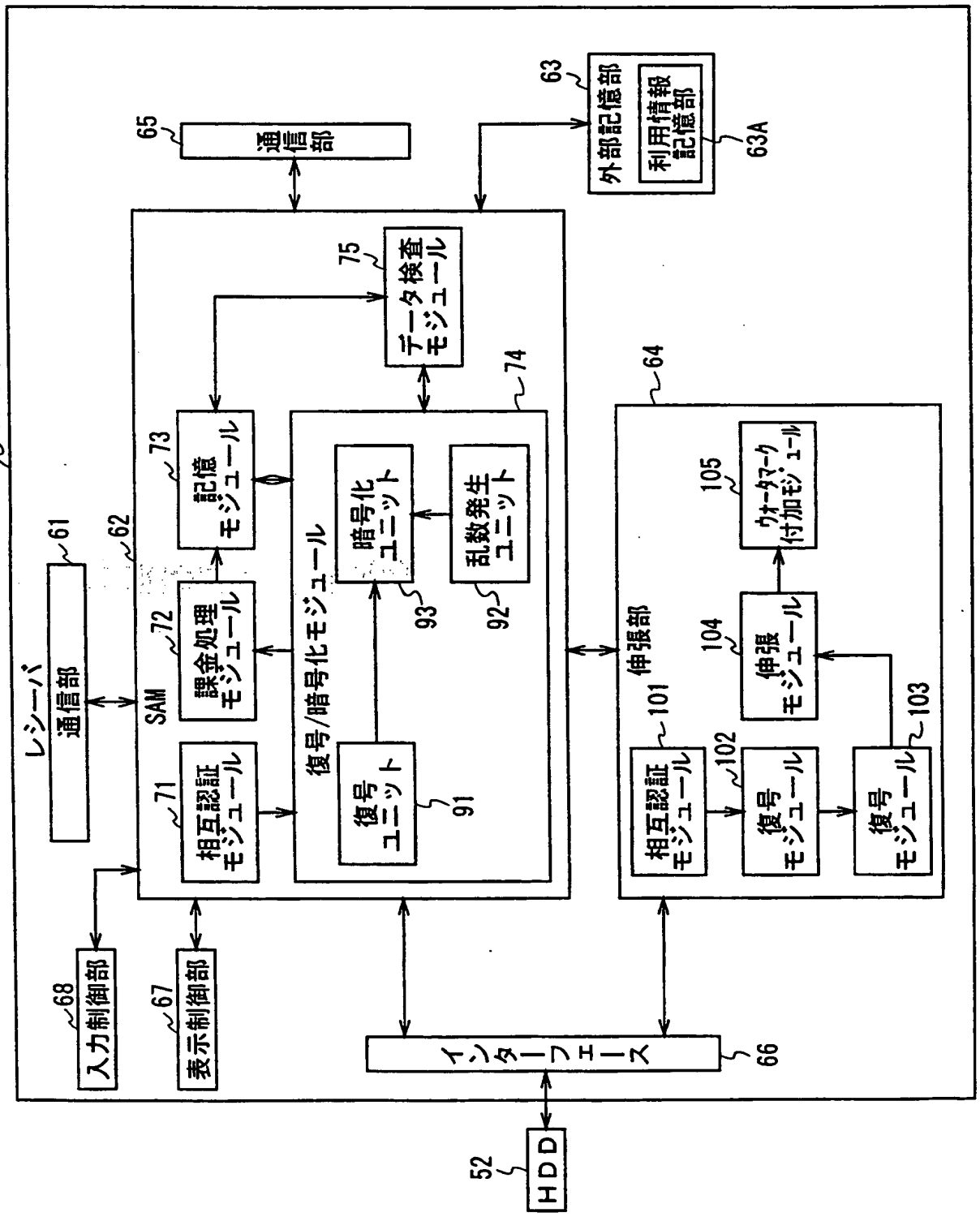

51 レシーバ
65 通信部
63 外部記憶部
利用情報記憶部
63A
75 データ検査モジュール
74
64
73 記憶モジュール
61
62
暗号化ユニット
乱数発生ユニット
105 ウォータマーク付加モジュール
レシーバ通信部
SAM
72 課金処理モジュール
93
92
復号/暗号化モジュール
伸張部
104 伸張モジュール
71 相互認証モジュール
復号ユニット
91
101 相互認証モジュール
102 復号モジュール
103 復号モジュール
68 入力制御部
67 表示制御部
インターフェース
66
52 HDD

図26

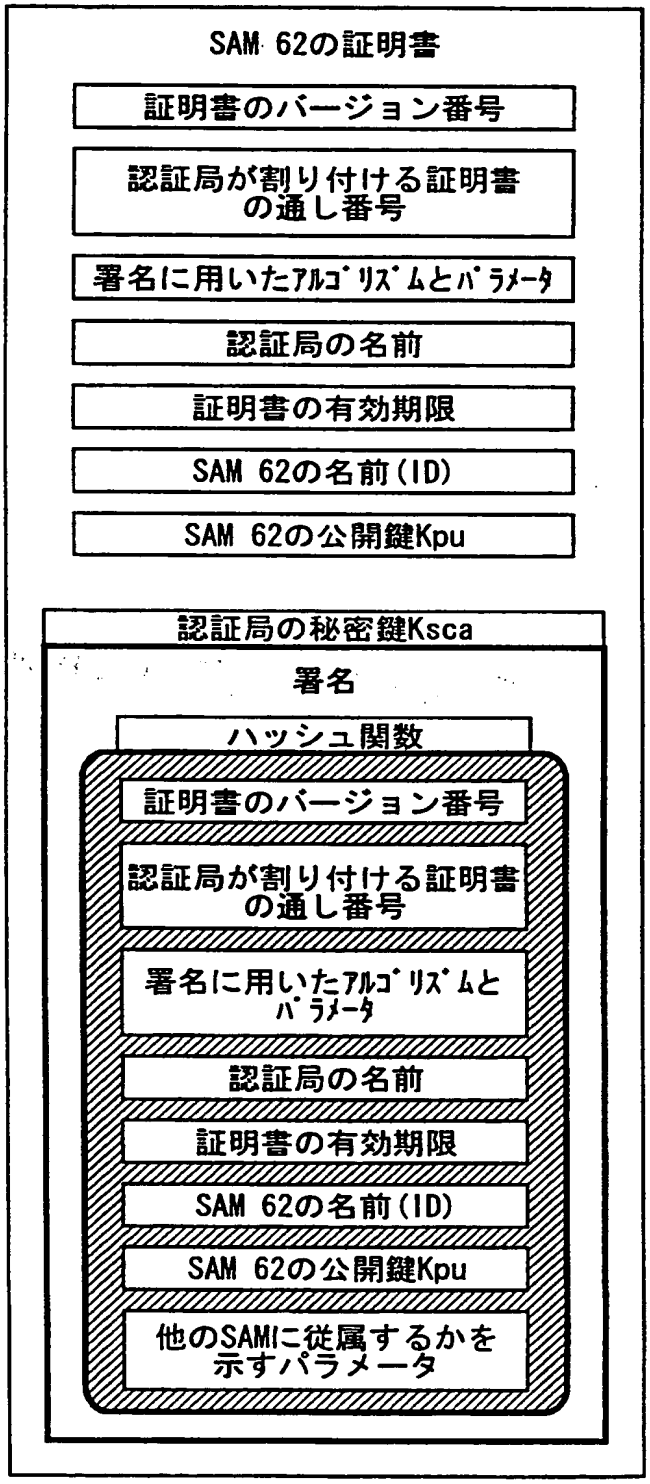

SAM 62の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
SAM 62の名前(ID)
SAM 62の公開鍵Kpu
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
SAM 62の名前(ID)
SAM 62の公開鍵Kpu
他のSAMに従属するかを示すパラメータ

図２７

コンテンツのID		コンテンツAのID
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID		ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID		ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		UCSAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容 11のID
	形式	買い取り再生
	パラメータ	×××
	管理移動状態情報	管理移動元:SAM62のID、 管理移動先:SAM62のID
利用履歴		×××

UCSA

図２８

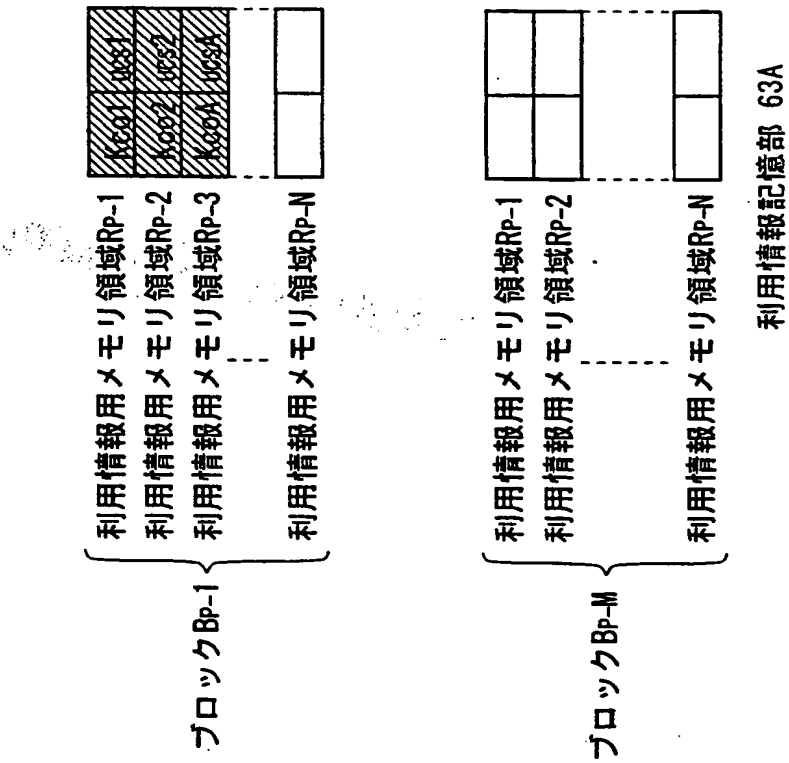

利用情報用メモリ領域RP-1
利用情報用メモリ領域RP-2
利用情報用メモリ領域RP-3
利用情報用メモリ領域RP-N
ブロックBP-1
利用情報用メモリ領域RP-1
利用情報用メモリ領域RP-2
利用情報用メモリ領域RP-N
ブロックBP-M
利用情報記憶部 63A

図29

コンテンツのID		コンテンツAのID
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID		ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID		ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		UCSAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容11のID
	形式	買い取り再生
	パラメータ	×××
	管理移動状態情報	管理移動元:SAM62のID、 管理移動先:SAM62のID
課金履歴		×××

課金情報 A

図３０

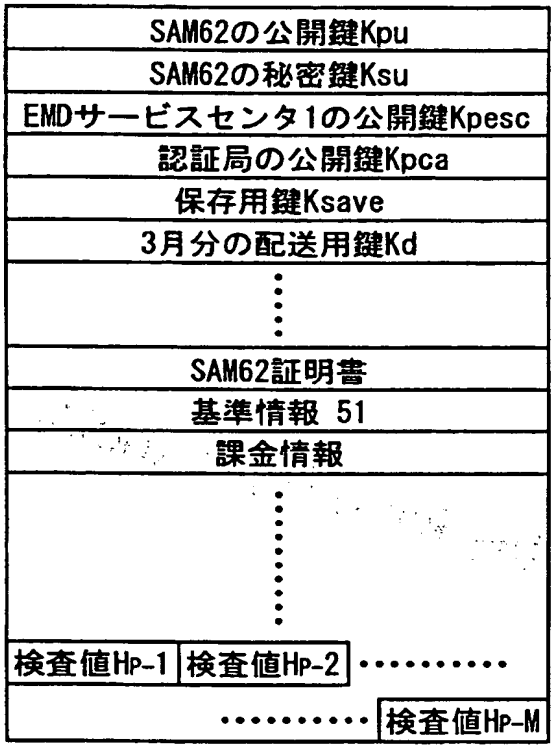

SAM62の公開鍵Kpu
SAM62の秘密鍵Ksu
EMDサービスセンタ1の公開鍵Kpesc
認証局の公開鍵Kpca
保存用鍵Ksave
3月分の配送用鍵Kd
SAM62証明書
基準情報 51
課金情報
検査値Hp-1
検査値Hp-2
検査値Hp-M

図３１

SAMのID		SAM62のID
機器番号		ﾚｼｰﾊﾞ51の機器番号 (100番)
決済ID		ユーザFの決済ID
課金の上限額		正式登録時の 課金の上限額
決済ユーザ情報	氏名	ユーザFの氏名
	住所	ユーザFの住所
	電話番号	ユーザFの電話番号
	決済機関情報	ユーザFの決済機関情報
	生年月日	ユーザFの生年月日
	年齢	ユーザFの年齢(21才)
	性別	ユーザFの性別(男)
	ユーザのID	ユーザFのID
	パスワード	ユーザFのパスワード
従属ユーザ情報	氏名	
	住所	
	電話番号	
	生年月日	
	性別	
	ユーザのID	
	パスワード	
⋮		
利用ﾎﾟｲﾝﾄ情報		ﾚｼｰﾊﾞ51の利用 ﾎﾟｲﾝﾄ情報

基準情報 51

図３２

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ 2-1	222ポイント
	コンテンツプロバイダ 2-2	123ポイント
	サービスプロバイダ 3-1	345ポイント
	サービスプロバイダ 3-2	0ポイント

基準情報51の利用ポイント情報

図３３

	SAM ID	ユーザID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リスト署名
レシーバ51の登録条件	SAM62のID	ユーザFのID	可	可	SAM62のID	なし	制限なし	××××	××××
レシーバ201の登録リスト	SAM212のID	ユーザAのID	可	可	SAM212のID	なし	制限なし	××××	

リスト部

対象SAM ID	SAM62のID
有効期限	××××
バージョン番号	××××
接続されている機器数	2

対象SAM情報部

図３４

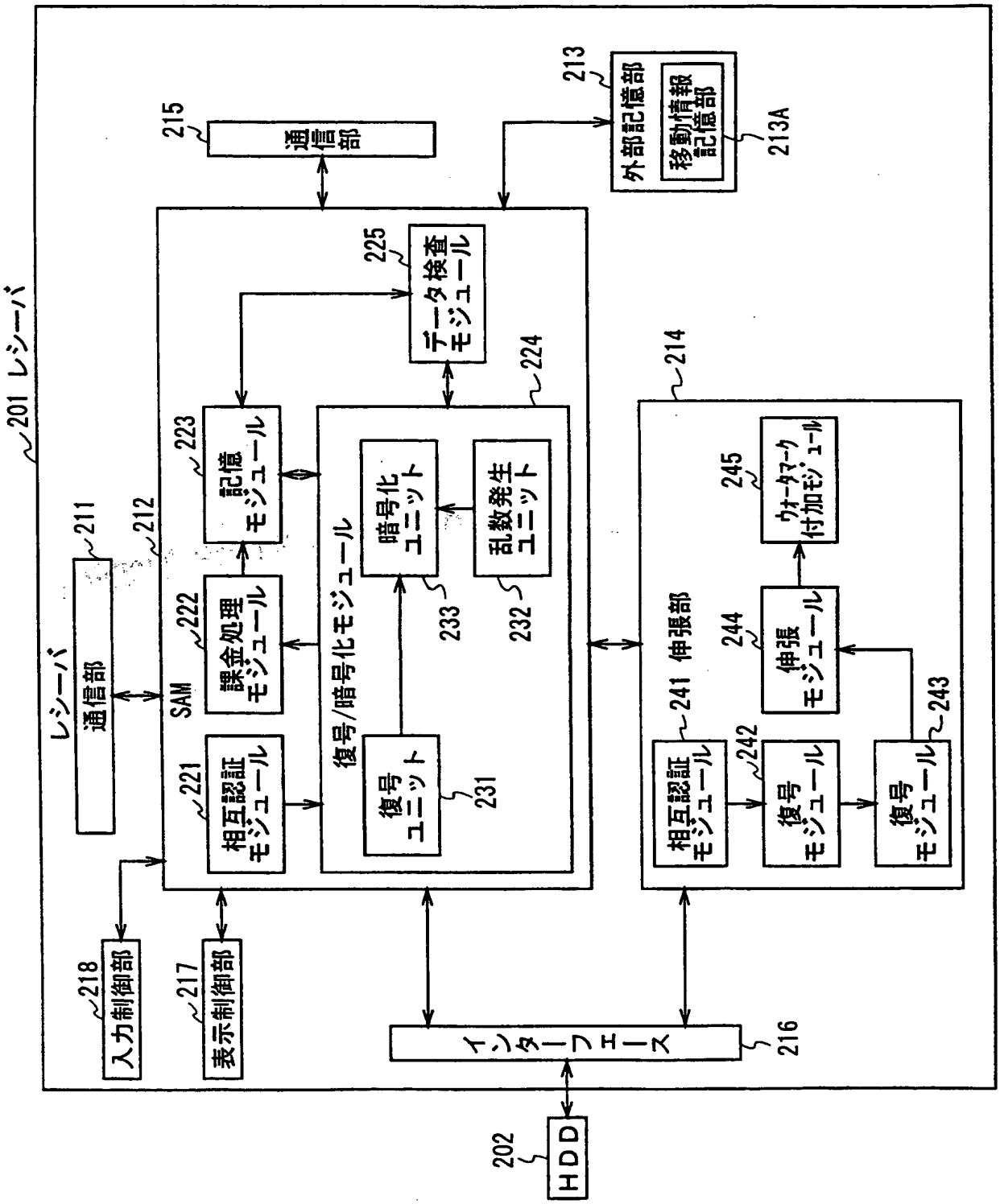

201 レシーバ
215 通信部
213 外部記憶部
213A 移動情報記憶部
225 データ検査モジュール
224
214
223 記憶モジュール
暗号化ユニット
乱数発生ユニット
245 ウォータマーク付加モジュール
211
212
レシーバ
通信部
SAM
222 課金処理モジュール
復号/暗号化モジュール
233
232
244 伸張モジュール
241 伸張部
243
221 相互認証モジュール
復号ユニット
231
242
相互認証モジュール
復号モジュール
復号モジュール
218 入力制御部
217 表示制御部
インターフェース
216
202
HDD

図35

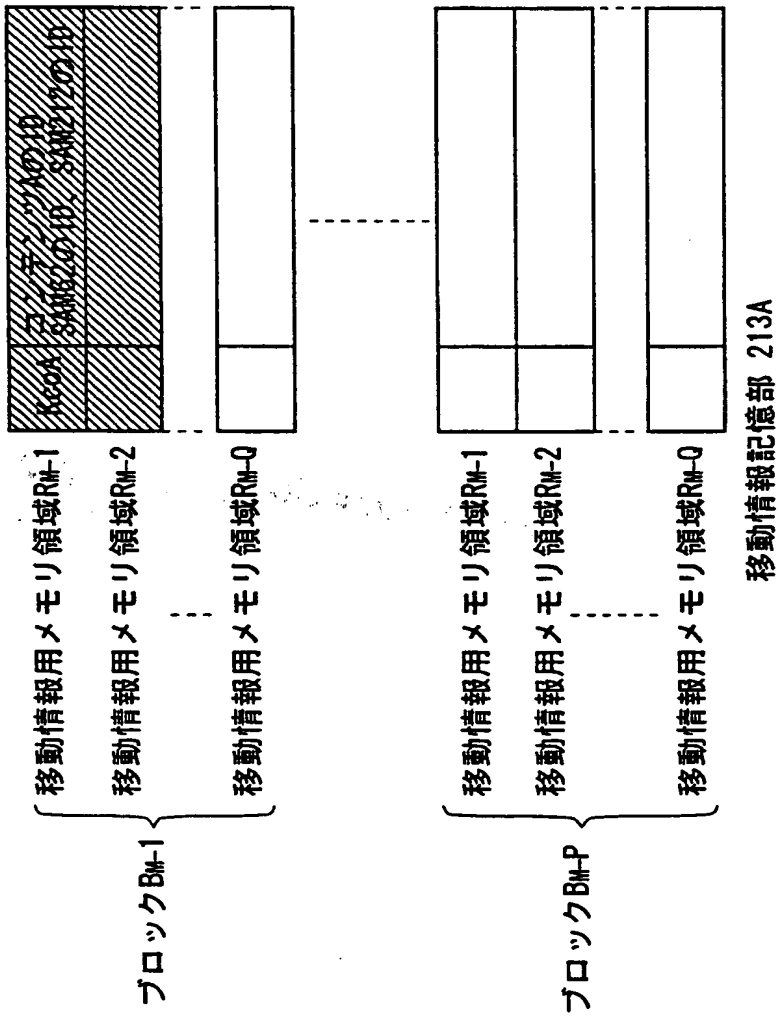

移動情報用メモリ領域RM-1
移動情報用メモリ領域RM-2
移動情報用メモリ領域RM-0
ブロックBM-1
移動情報用メモリ領域RM-1
移動情報用メモリ領域RM-2
移動情報用メモリ領域RM-0
ブロックBM-P
移動情報記憶部 213A

図３６

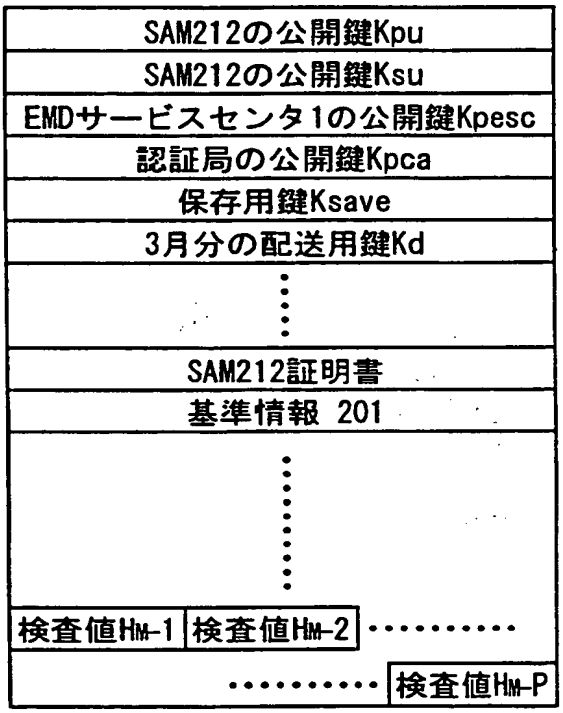

SAM212の公開鍵Kpu
SAM212の公開鍵Ksu
EMDサービスセンタ1の公開鍵Kpesc
認証局の公開鍵Kpca
保存用鍵Ksave
3月分の配送用鍵Kd
SAM212証明書
基準情報 201
検査値HM-1
検査値HM-2
検査値HM-P

図３７

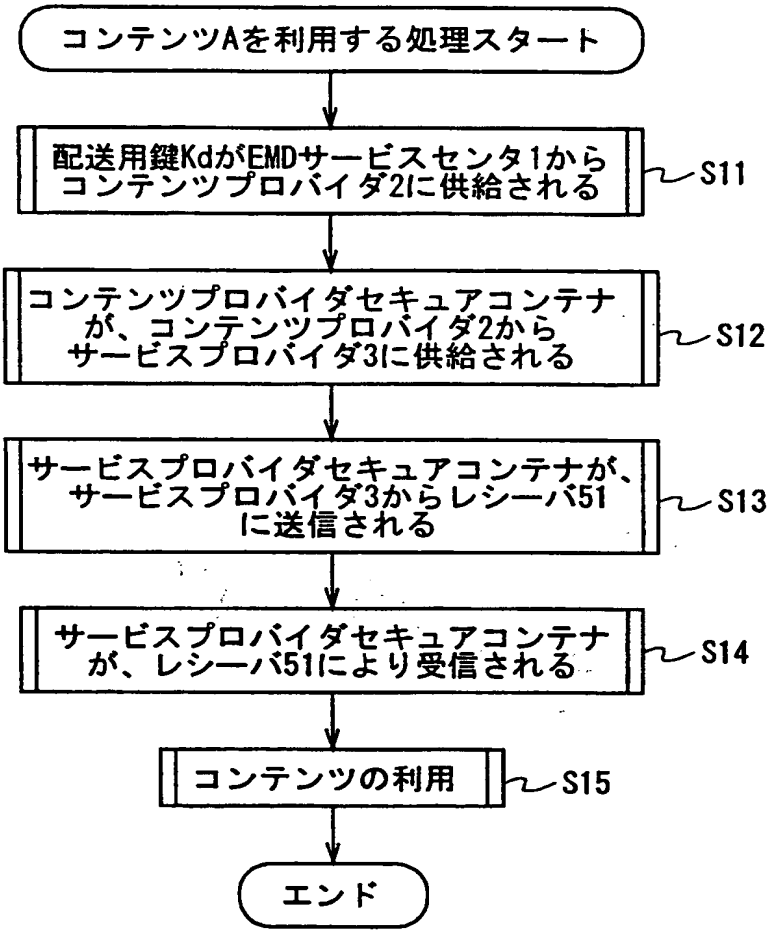

コンテンツAを利用する処理スタート
配送用鍵KdがEMDサービスセンタ1から
コンテンツプロバイダ2に供給される
S11
コンテンツプロバイダセキュアコンテナ
が、コンテンツプロバイダ2から
サービスプロバイダ3に供給される
S12
サービスプロバイダセキュアコンテナが、
サービスプロバイダ3からレシーバ51
に送信される
S13
サービスプロバイダセキュアコンテナ
が、レシーバ51により受信される
S14
コンテンツの利用
S15
エンド

図３８

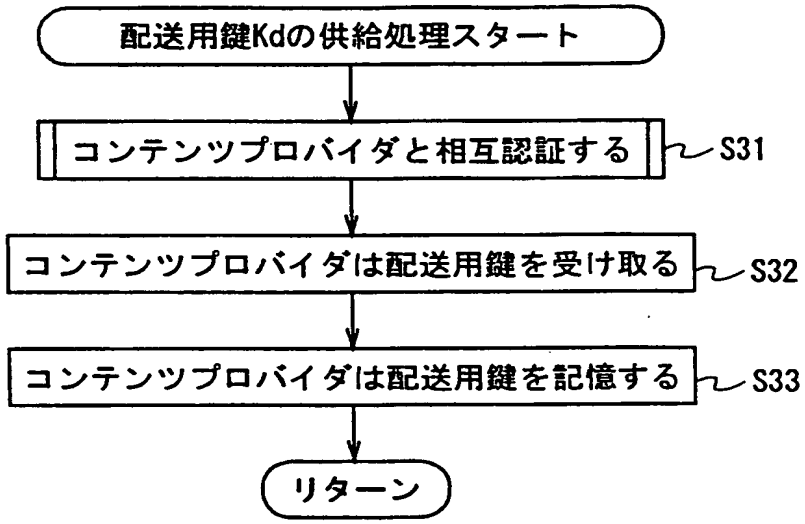

配送用鍵Kdの供給処理スタート
コンテンツプロバイダと相互認証する
S31
コンテンツプロバイダは配送用鍵を受け取る
S32
コンテンツプロバイダは配送用鍵を記憶する
S33
リターン

図３９

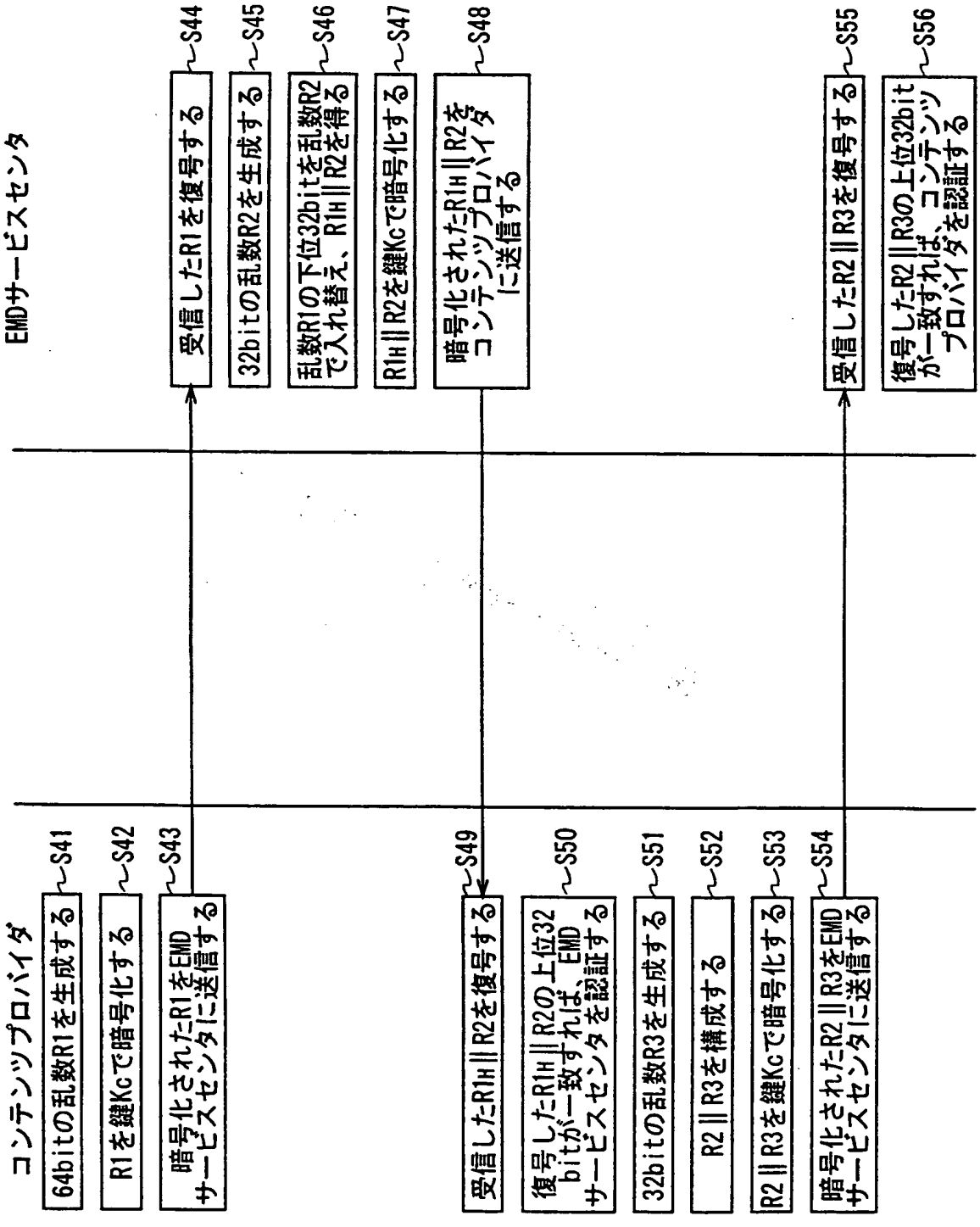

コンテンツプロバイダ
EMDサービスセンタ
64bitの乱数R1を生成する
S41
R1を鍵Kcで暗号化する
S42
暗号化されたR1をEMD サービスセンタに送信する
S43
受信したR1を復号する
S44
32bitの乱数R2を生成する
S45
乱数R1の下位32bitを乱数R2で入れ替え、R1H||R2を得る
S46
R1H||R2を鍵Kcで暗号化する
S47
暗号化されたR1H||R2をコンテンツプロバイダに送信する
S48
受信したR1H||R2を復号する
S49
復号したR1H||R2の上位32bitが一致すれば、EMDサービスセンタを認証する
S50
32bitの乱数R3を生成する
S51
R2||R3を構成する
S52
R2||R3を鍵Kcで暗号化する
S53
暗号化されたR2||R3をEMDサービスセンタに送信する
S54
受信したR2||R3を復号する
S55
復号したR2||R3の上位32bitが一致すれば、コンテンツプロバイダを認証する
S56

図40

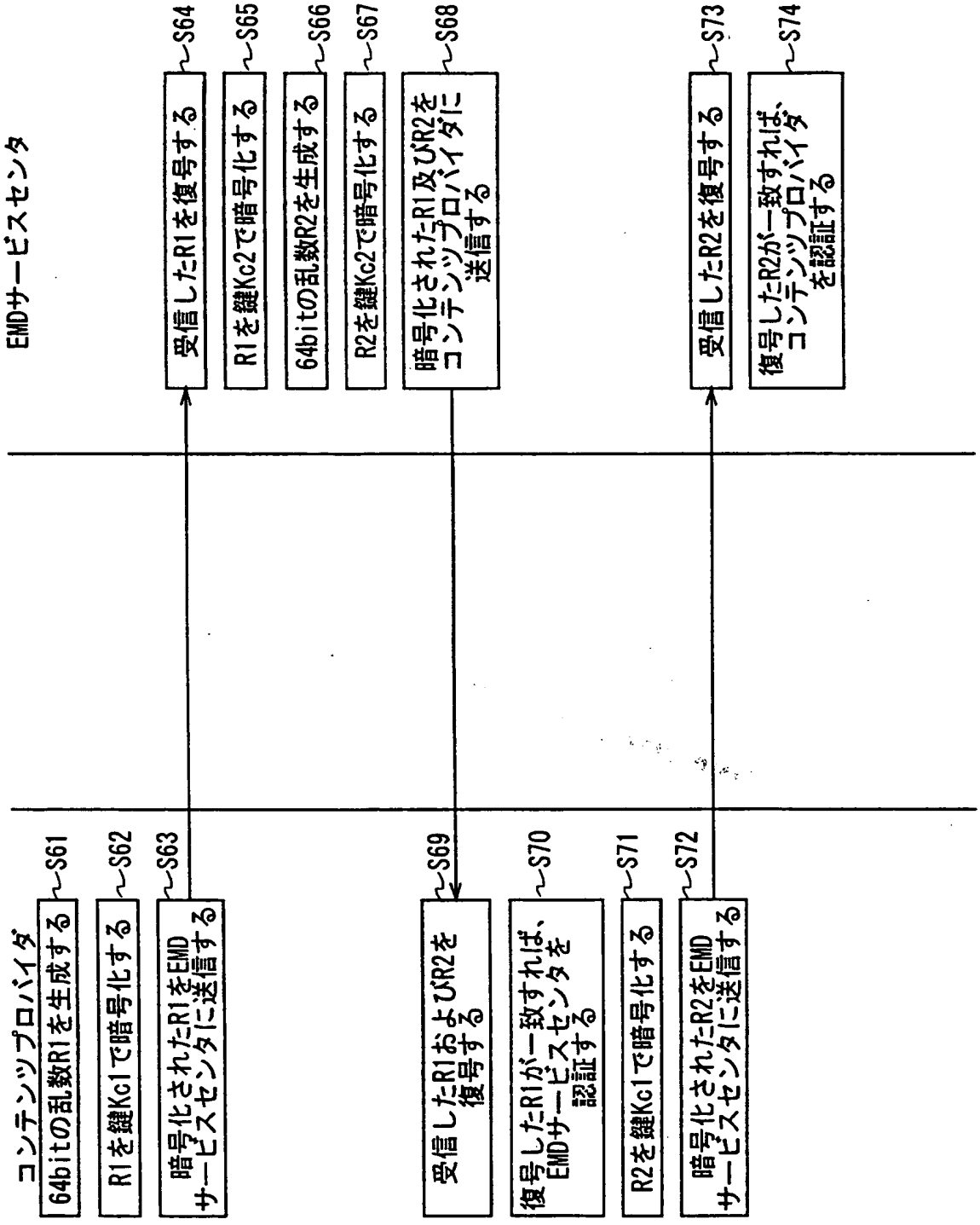

コンテンツプロバイダ
EMDサービスセンタ
64bitの乱数R1を生成する
S61
R1を鍵Kc1で暗号化する
S62
暗号化されたR1をEMD サービスセンタに送信する
S63
受信したR1を復号する
S64
R1を鍵Kc2で暗号化する
S65
64bitの乱数R2を生成する
S66
R2を鍵Kc2で暗号化する
S67
暗号化されたR1及びR2を コンテンツプロバイダに 送信する
S68
受信したR1および R2を 復号する
S69
復号したR1が一致すれば、 EMDサービスセンタを 認証する
S70
R2を鍵Kc1で暗号化する
S71
暗号化されたR2をEMD サービスセンタに送信する
S72
受信したR2を復号する
S73
復号したR2が一致すれば、 コンテンツプロバイダ を認証する
S74

図41

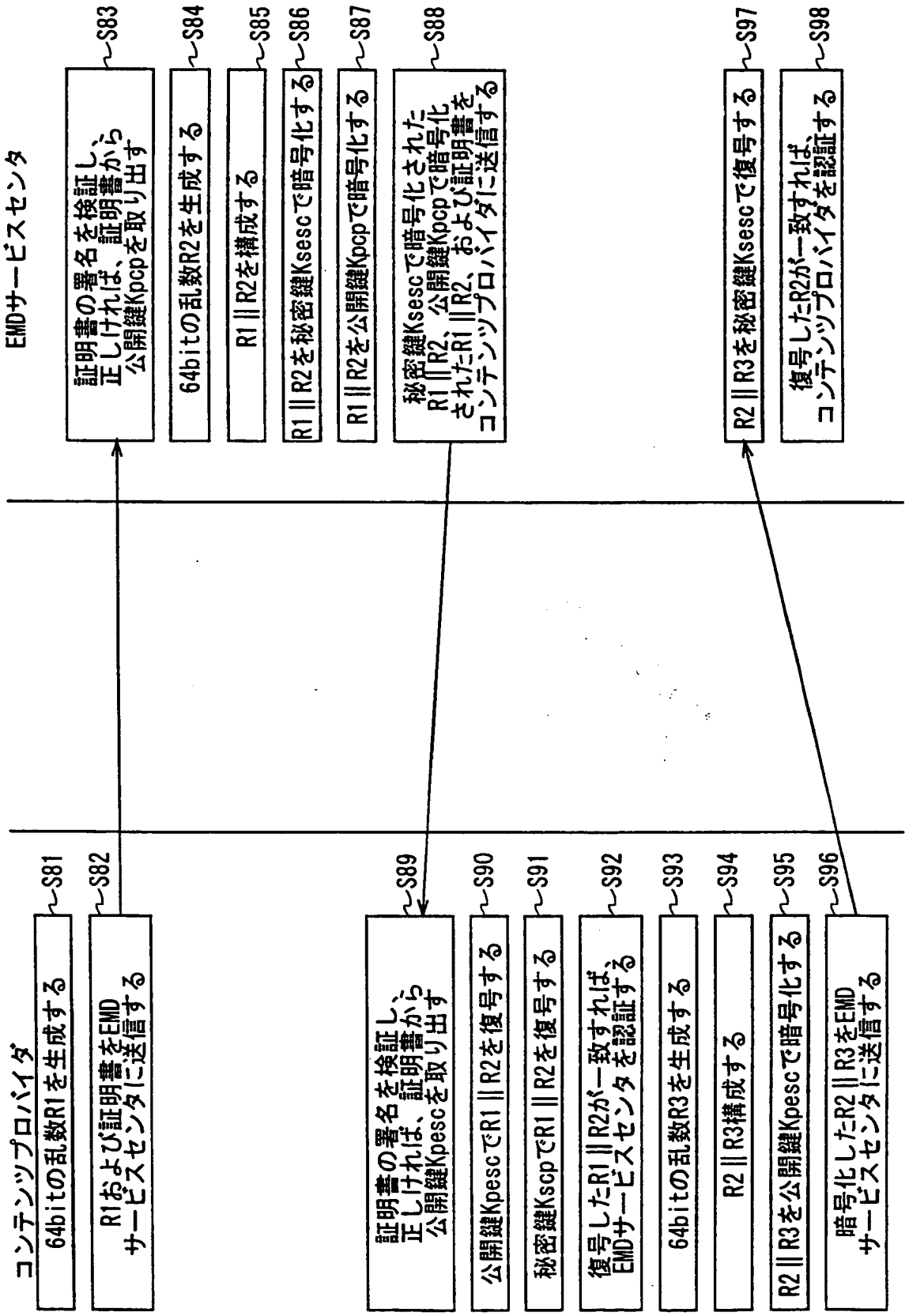

コンテンツプロバイダ
64bitの乱数R1を生成する
S81
R1および証明書をEMD
サービスセンタに送信する
S82
EMDサービスセンタ
証明書の署名を検証し、
正しければ、証明書から
公開鍵Kpcpを取り出す
S83
64bitの乱数R2を生成する
S84
R1 || R2を構成する
S85
R1 || R2を秘密鍵Ksescで暗号化する
S86
R1 || R2を公開鍵Kpcpで暗号化する
S87
秘密鍵Ksescで暗号化された
R1 || R2、公開鍵Kpcpで暗号化
されたR1 || R2、および証明書を
コンテンツプロバイダに送信する
S88
証明書の署名を検証し、
正しければ、証明書から
公開鍵Kpescを取り出す
S89
公開鍵KpescでR1 || R2を復号する
S90
秘密鍵KscpでR1 || R2を復号する
S91
復号したR1 || R2が一致すれば、
EMDサービスセンタを認証する
S92
64bitの乱数R3を生成する
S93
R2 || R3構成する
S94
R2 || R3を公開鍵Kpescで暗号化する
S95
暗号化したR2 || R3をEMD
サービスセンタに送信する
S96
R2 || R3を秘密鍵Ksescで復号する
S97
復号したR2が一致すれば、
コンテンツプロバイダを認証する
S98

図４２

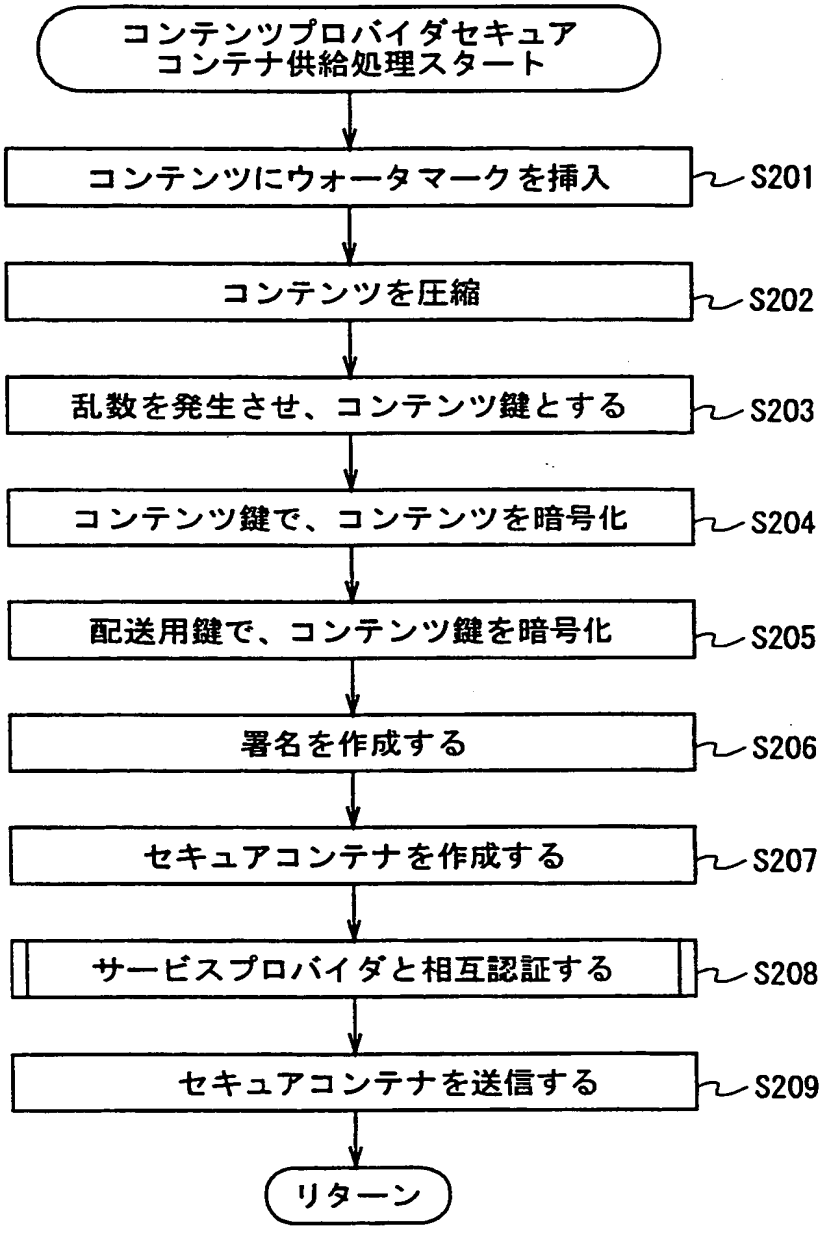

コンテンツプロバイダセキュア
コンテナ供給処理スタート
コンテンツにウォータマークを挿入
S201
コンテンツを圧縮
S202
乱数を発生させ、コンテンツ鍵とする
S203
コンテンツ鍵で、コンテンツを暗号化
S204
配送用鍵で、コンテンツ鍵を暗号化
S205
署名を作成する
S206
セキュアコンテナを作成する
S207
サービスプロバイダと相互認証する
S208
セキュアコンテナを送信する
S209
リターン

図４３

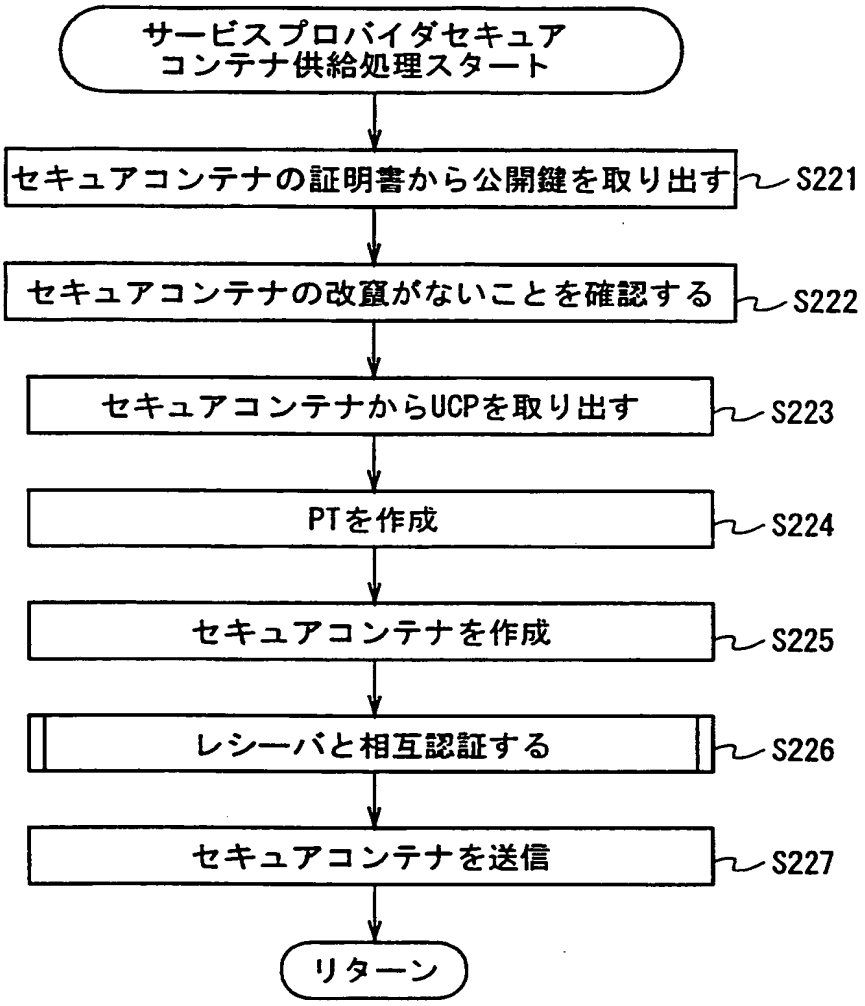

サービスプロバイダセキュア
コンテナ供給処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S221
セキュアコンテナの改竄がないことを確認する
S222
セキュアコンテナからUCPを取り出す
S223
PTを作成
S224
セキュアコンテナを作成
S225
レシーバと相互認証する
S226
セキュアコンテナを送信
S227
リターン

図４４

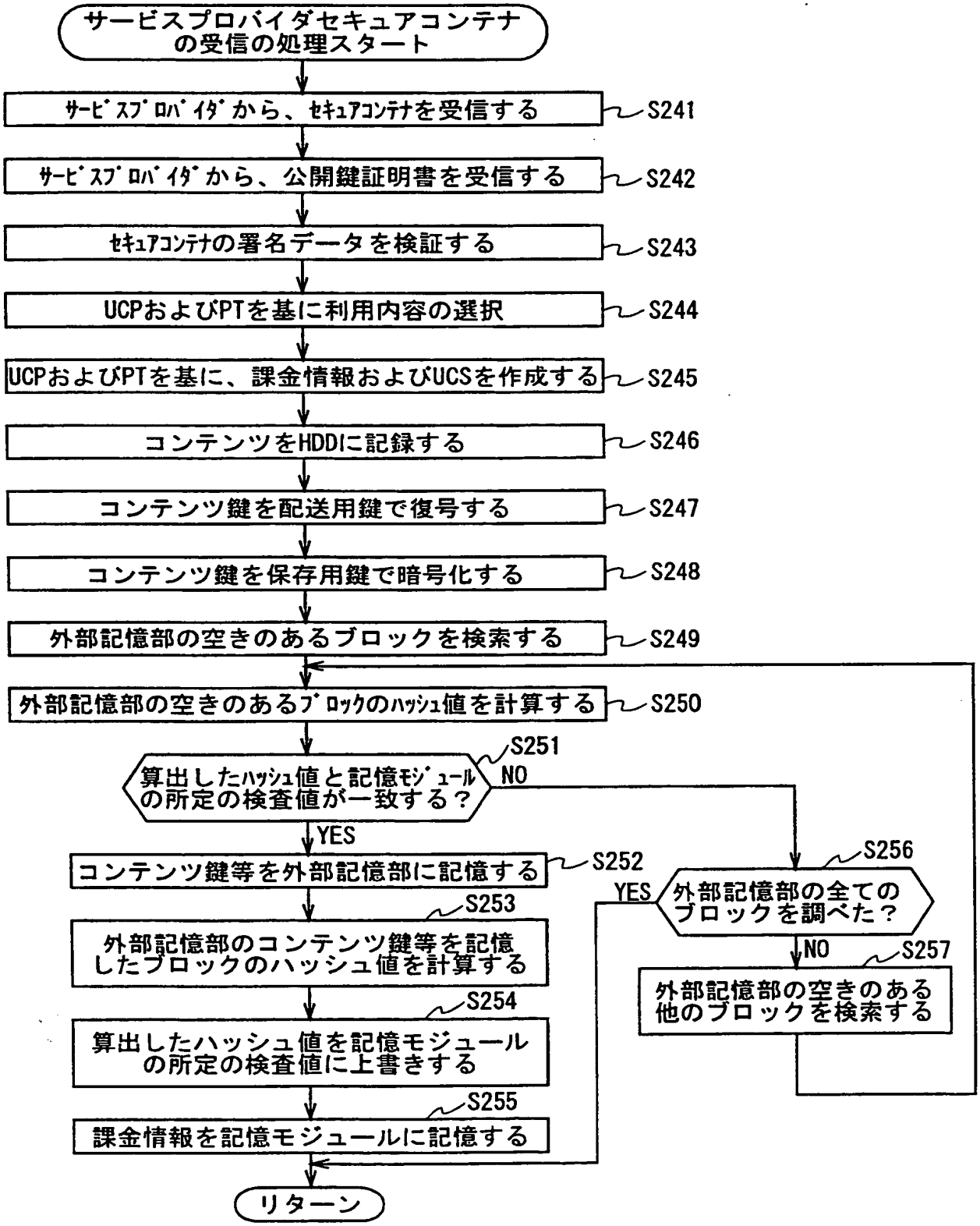

サービスプロバイダセキュアコンテナの受信の処理スタート
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞから、ｾｷｭｱｺﾝﾃﾅを受信する
S241
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞから、公開鍵証明書を受信する
S242
ｾｷｭｱｺﾝﾃﾅの署名データを検証する
S243
UCPおよびPTを基に利用内容の選択
S244
UCPおよびPTを基に、課金情報およびUCSを作成する
S245
コンテンツをHDDに記録する
S246
コンテンツ鍵を配送用鍵で復号する
S247
コンテンツ鍵を保存用鍵で暗号化する
S248
外部記憶部の空きのあるブロックを検索する
S249
外部記憶部の空きのあるﾌﾞﾛｯｸのﾊｯｼｭ値を計算する
S250
S251
算出したﾊｯｼｭ値と記憶ﾓｼﾞｭｰﾙの所定の検査値が一致する？
NO
YES
コンテンツ鍵等を外部記憶部に記憶する
S252
S253
外部記憶部のコンテンツ鍵等を記憶したブロックのハッシュ値を計算する
S254
算出したハッシュ値を記憶モジュールの所定の検査値に上書きする
S255
課金情報を記憶モジュールに記憶する
S256
YES
外部記憶部の全てのブロックを調べた？
NO
S257
外部記憶部の空きのある他のブロックを検索する
リターン

図４５

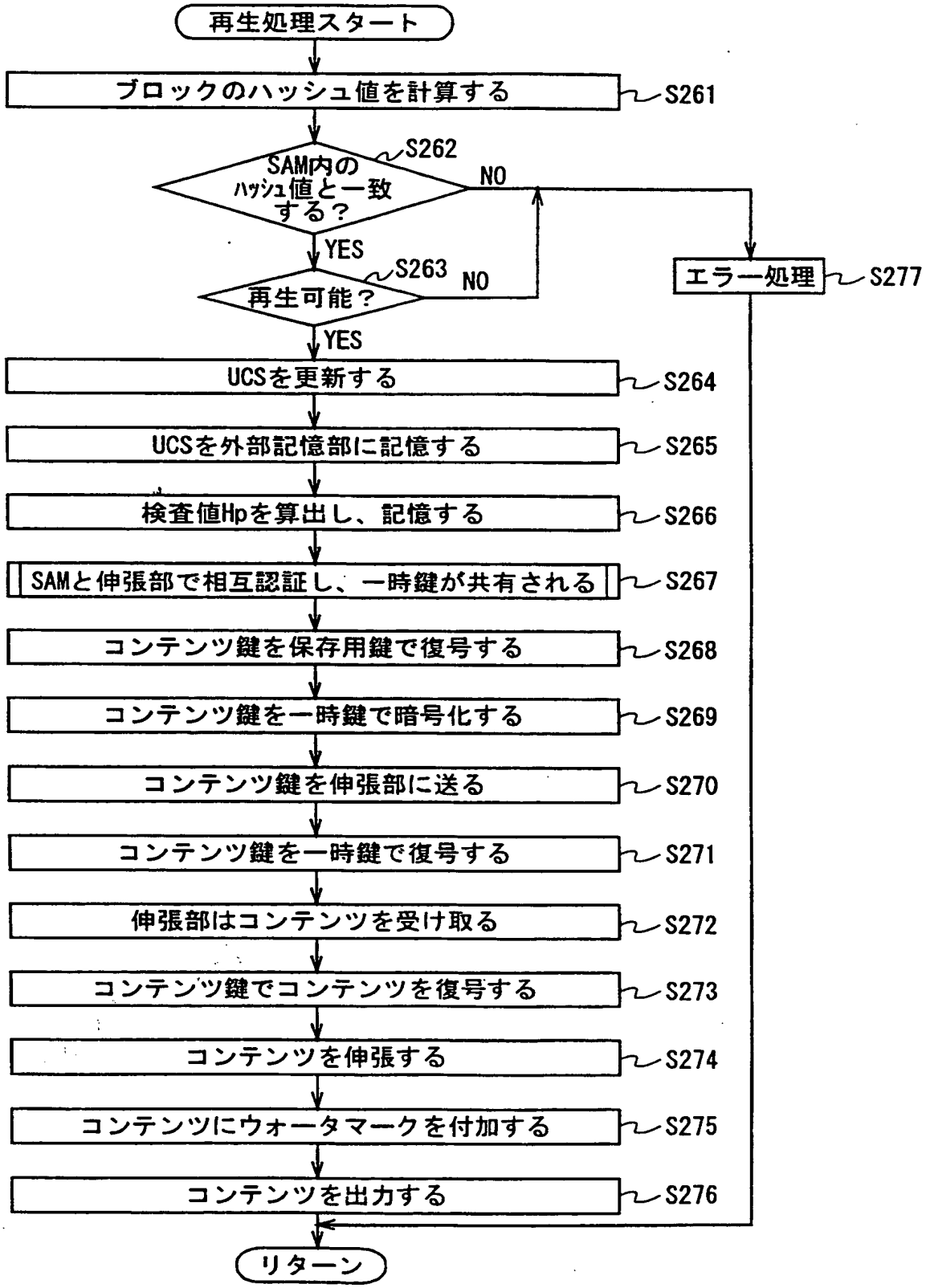

再生処理スタート
ブロックのハッシュ値を計算する
S261
SAM内のハッシュ値と一致する？
S262
NO
YES
再生可能？
S263
NO
エラー処理
S277
YES
UCSを更新する
S264
UCSを外部記憶部に記憶する
S265
検査値Hpを算出し、記憶する
S266
SAMと伸張部で相互認証し、一時鍵が共有される
S267
コンテンツ鍵を保存用鍵で復号する
S268
コンテンツ鍵を一時鍵で暗号化する
S269
コンテンツ鍵を伸張部に送る
S270
コンテンツ鍵を一時鍵で復号する
S271
伸張部はコンテンツを受け取る
S272
コンテンツ鍵でコンテンツを復号する
S273
コンテンツを伸張する
S274
コンテンツにウォータマークを付加する
S275
コンテンツを出力する
S276
リターン

図４６

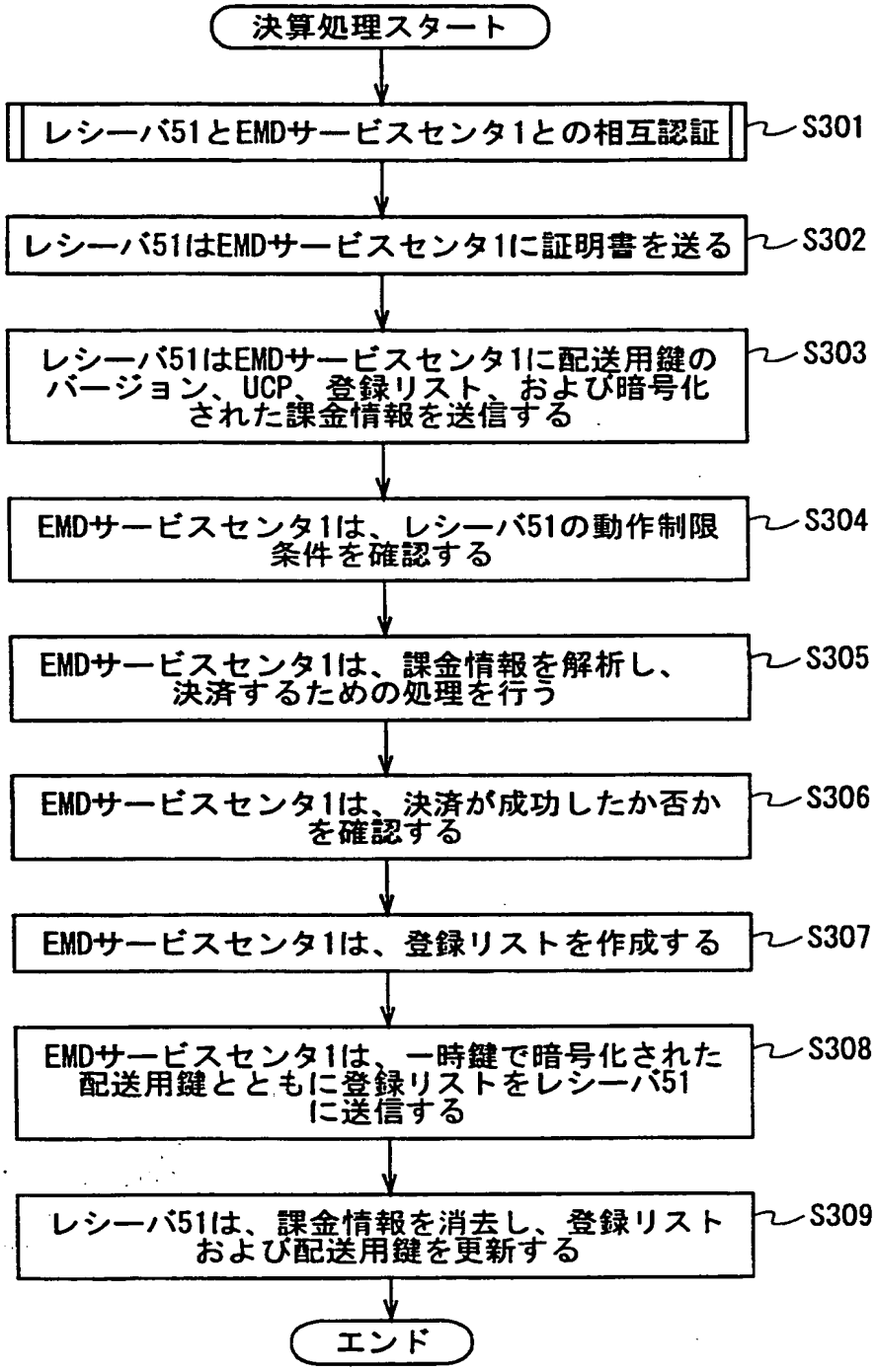

決算処理スタート
レシーバ51とEMDサービスセンタ1との相互認証
S301
レシーバ51はEMDサービスセンタ1に証明書を送る
S302
レシーバ51はEMDサービスセンタ1に配送用鍵のバージョン、UCP、登録リスト、および暗号化された課金情報を送信する
S303
EMDサービスセンタ1は、レシーバ51の動作制限条件を確認する
S304
EMDサービスセンタ1は、課金情報を解析し、決済するための処理を行う
S305
EMDサービスセンタ1は、決済が成功したか否かを確認する
S306
EMDサービスセンタ1は、登録リストを作成する
S307
EMDサービスセンタ1は、一時鍵で暗号化された配送用鍵とともに登録リストをレシーバ51に送信する
S308
レシーバ51は、課金情報を消去し、登録リストおよび配送用鍵を更新する
S309
エンド

図４７

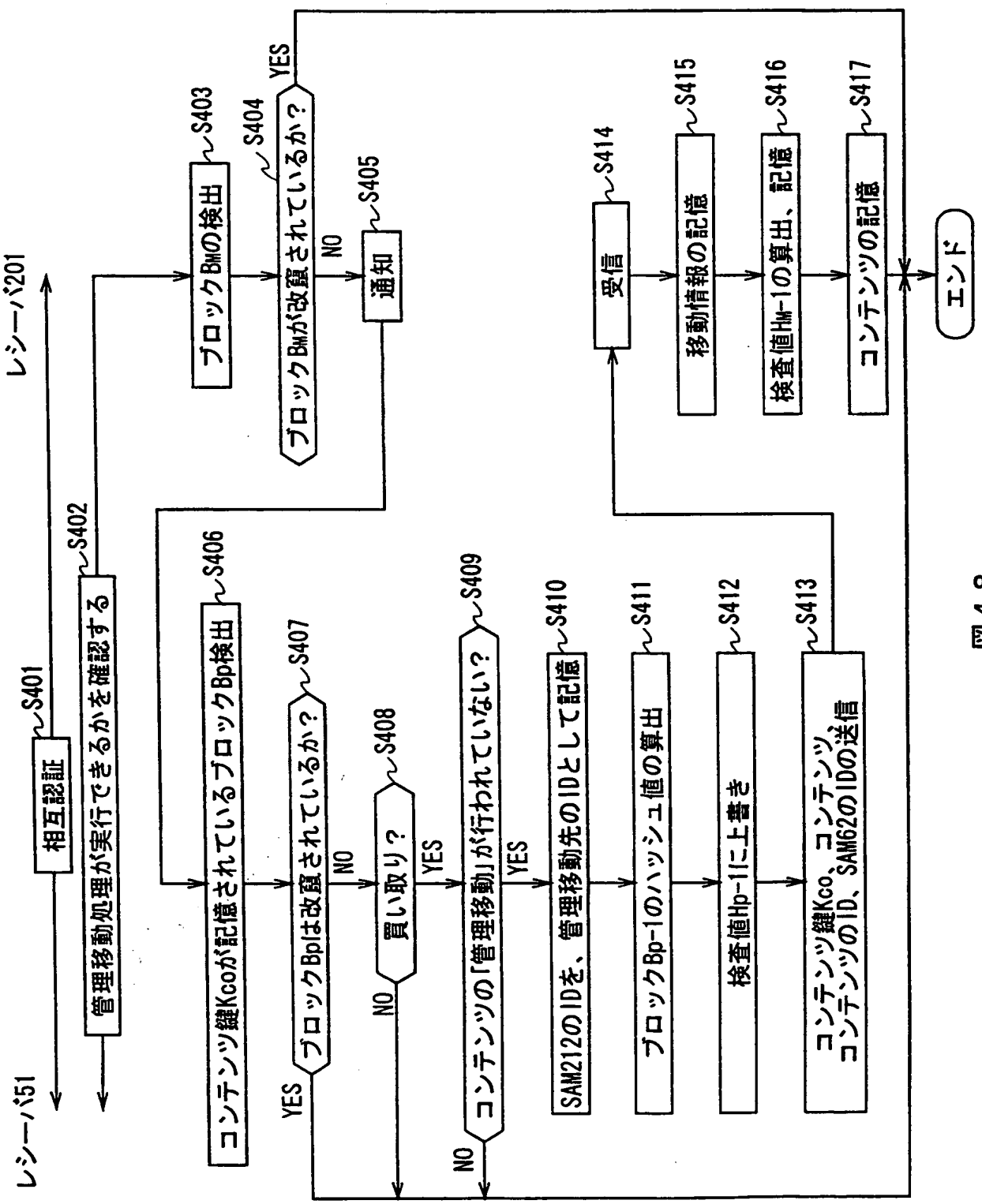

レシーバ201
レシーバ51
S401
相互認証
S402
管理移動処理が実行できるかを確認する
S403
ブロックBMの検出
S404
ブロックBMが改竄されているか？
YES
NO
S405
通知
S406
コンテンツ鍵Kcoが記憶されているブロックBp検出
S407
ブロックBpは改竄されているか？
YES
NO
S408
買い取り？
NO
YES
S409
コンテンツの「管理移動」が行われていない？
NO
YES
S410
SAM212のIDを、管理移動先のIDとして記憶
S411
ブロックBp-1のハッシュ値の算出
S412
検査値Hp-1に上書き
S413
コンテンツ鍵Kco、コンテンツ、
コンテンツのID、SAM62のIDの送信
S414
受信
S415
移動情報の記憶
S416
検査値HM-1の算出、記憶
S417
コンテンツの記憶
エンド

図48

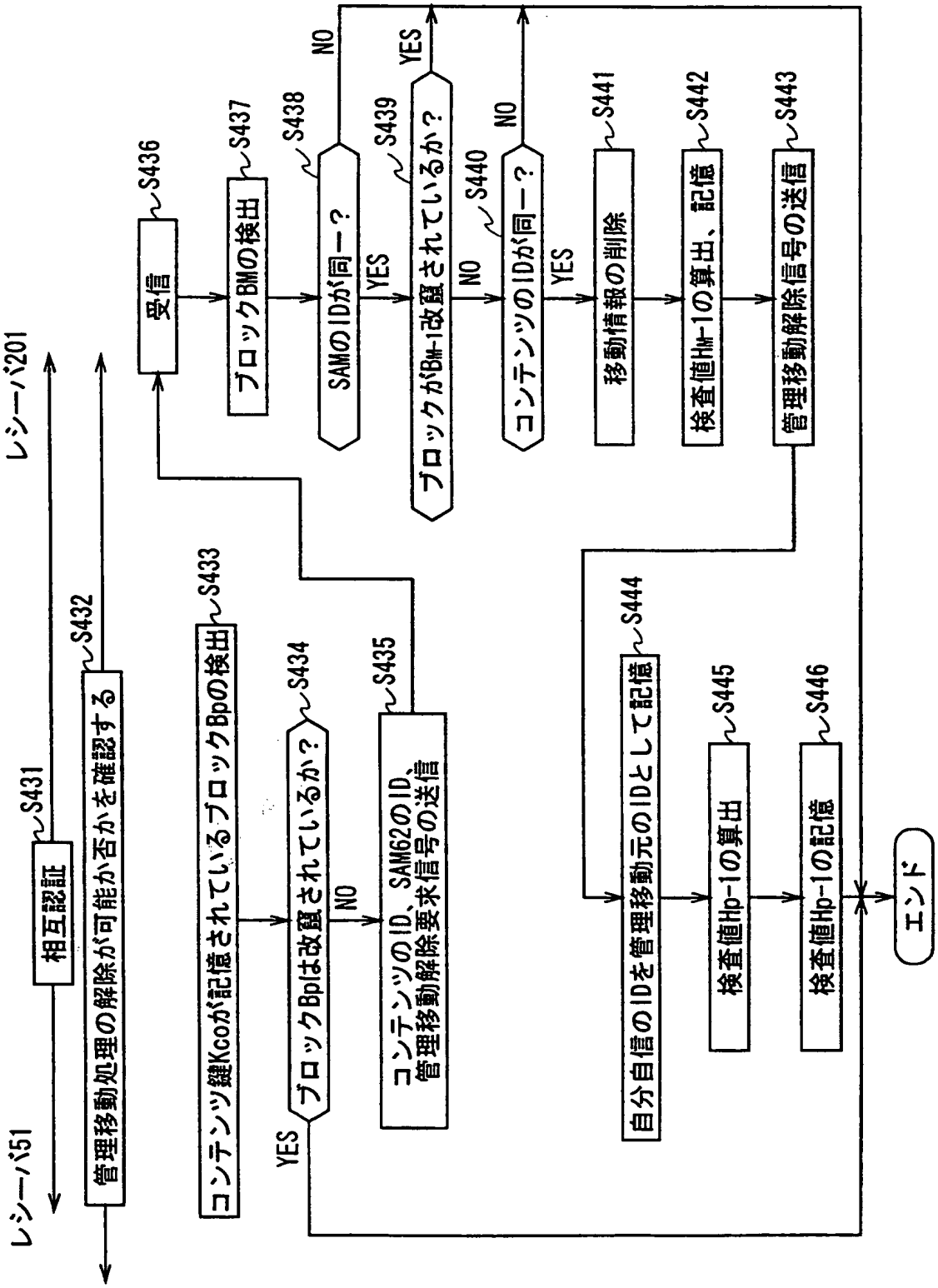

レシーバ201
レシーバ51
相互認証
S431
管理移動処理の解除が可能か否かを確認する
S432
コンテンツ鍵Kcoが記憶されているブロックBpの検出
S433
ブロックBpは改竄されているか？
S434
YES
NO
コンテンツのID、SAM62のID、管理移動解除要求信号の送信
S435
受信
S436
ブロックBMの検出
S437
SAMのIDが同一？
S438
NO
YES
ブロックがBM-1改竄されているか？
S439
YES
NO
コンテンツのIDが同一？
S440
NO
YES
移動情報の削除
S441
検査値HM-1の算出、記憶
S442
管理移動解除信号の送信
S443
自分自信のIDを管理移動元のIDとして記憶
S444
検査値Hp-1の算出
S445
検査値Hp-1の記憶
S446
エンド

図49

符　号　の　説　明

１．．．ＥＭＤサービスセンタ，２．．．コンテンツプロバイダ，３．．．サービスプロバイダ，５．．．ユーザホームネットワーク，１１．．．サービスプロバイダ管理部，１２．．．コンテンツプロバイダ管理部，１３．．．著作権管理部，１４．．．鍵サーバ，１５．．．経歴データ管理部，１６．．．利益分配部，１７．．．相互認証部，１８．．．ユーザ管理部，１９．．．課金請求部，２０．．．出納部，２１．．．監査部，３１．．．コンテンツサーバ，３２．．．ウォータマーク付加部，３３．．．圧縮部，３４．．．暗号化部，３５．．．乱数発生部，３６．．．暗号化部，３７．．．ポリシー記憶部，３８．．．セキュアコンテナ作成部，３９．．．相互認証部，４１．．．　コンテンツサーバ，４２．．．値付け部，４３．．．ポリシー記憶部，４４．．．セキュアコンテナ作成部，４５．．．相互認証部，５１．．．レシーバ，５２．．．ＨＤＤ，６１．．．通信部，６２．．．ＳＡＭ，６３．．．外部記憶部，６４．．．伸張部，６５．．．通信部，６６．．．インタフェース，６７．．．表示制御部，６８．．．入力制御部，７１．．．相互認証モジュール，７２．．．課金処理モジュール，７３．．．記憶モジュール，７４．．．復号／暗号化モジュール，７５．．．データ検査モジュール，９１．．．復号ユニット，９２．．．乱数発生ユニット，９３．．．暗号化ユニット，１０１．．．相互認証モジュール，１０２．．．復号モジュール，１０３．．．復号モジュール，１０４．．．伸張モジュール，１０５．．．ウォータマーク付加モジュール，２０１．．．レシーバ，２０２．．．ＨＤＤ，２１１．．．通信部，２１２．．．ＳＡＭ，２１３．．．外部記憶部，２１４．．．伸張部，２１５．．．通信部，２１６．．．　インタフェース，２１７．．．表示制御部，２１８．．．入力制御部，２２１．．．相

互認証モジュール，２２２．．．課金処理モジュール，２２３．．．記憶モジュール，２２４．．．復号／暗号化モジュール，２２５．．．データ検査モジュール，２３１．．．復号ユニット，２３２．．．乱数発生ユニット，２３３．．．暗号化ユニット，２４１．．．相互認証モジュール，２４２．．．復号モジュール，２４３．．．復号モジュール，２４４．．．伸張モジュール，２４５．．．ウォータマーク付加モジュール

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02290

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F17/60, G06F13/00, G09C1/00, H04L9/08, G06F15/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST File (JOIS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO, 96/27155, A2 (InerTrust Technologies Corp.), 06 September, 1996 (06.09.96) & JP, 10-512074, A	1-8
Y	Jinbun Kagaku to Computer, Vols. 36 to 38, November, 1997, Seiji Kawahara, "Chosaku Ken Shori Gijutsu no Saikin no Doko", pp.43-48	1-8

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 May, 2000 (24.05.00)	13 June, 2000 (13.06 00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０２２９０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int. Cl' G06F17/60

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int. Cl' G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1926-1996年
日本国公開実用新案公報　1971-2000年
日本国実用新案登録公報　1996-2000年
日本国登録実用新案公報　1994-2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTファイル(JOIS)

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO,96/27155,A2(InerTrust Technologies Corp.)6.9月.1996(06.09.96)&JP,10-512074,A	1-8
Y	人文科学とコンピュータ，第36-8巻，11月.1997 河原正治「著作権処理技術の最近の動向」p.43-48	1-8

☐ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
24.05.00	13.06.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5L	9287
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	岩間　直純 電話番号　０３－３５８１－１１０１　内線　3562		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）